Tommi Heikkilä

Verkonhallintajärjestelmän suojaaminen IPSecin avulla

Tietotekniikan (tietoliikenne)
pro gradu -tutkielma
28.10.2002

Jyväskylän yliopisto
Tietotekniikan laitos

Tekijä: Tommi Heikkilä

Yhteystiedot: Survontie 46 A 14, 40520 Jyväskylä, tommihei@cc.jyu.fi

Työn nimi: Verkonhallintajärjestelmän suojaaminen IPSecin avulla

Title in English: Securing network management with IPSec

Työ: Pro gradu -tutkielma

Sivumäärä: 122

Linja: Tietoliikenne

Teettäjä: Jyväskylän yliopisto, tietotekniikan laitos

Avainsanat: Verkonhallinta, tietoturva, tietoliikenne, suojaaminen, reititin, IP, IPSec

Keywords: network management, security, telecommunication, router, IP, IPSec

Tiivistelmä:

Tietoturva on noussut ajankohtaiseksi aiheeksi viime vuosien lukuisten tietokonevirusepidemioiden myötä. Tutkimuksien mukaan tietoturvahyökkäysten lukumäärä on kasvanut ja yhä useammin hyökkäykset kohdistuvat verkon runkolaitteisiin. Tulevaisuuden verkossa asiakkailla on mahdollisuus vaikuttaa saamaansa palvelun laatuun. Tämä luo uusia haasteita verkonhallinnan palveluille ja tietoturvalle. Tässä tutkielmassa kerrotaan verkonhallintaan liittyvän tietoliikenteen suojaamisesta, mietitään mitä uhkia siihen kohdistuu ja miten niitä voidaan estää toteutumasta. Täydellistä suojaa on lähes mahdoton tarjota, mutta tutkielmassa kuvataan keinoja, joilla riskit voidaan minimoida. Tutkielman pääpaino on verkonhallinta-aseman ja reitittimien välisen liikenteen turvaamisessa. Kokonaiskuvan muodostamiseksi tutkielmassa rakennetaan ensin malli organisaation verkon tietoturvalle ja käsitellään sitten tarkemmin verkonhallinnan osuus siitä. Mallissa hallintatieto liikkuu aina salattuna ja todennettuna, joten liikenne on turvassa passiivisilta hyökkäyksiltä ja tiedon muuntamiselta. Tutkielmassa esitetään eräs käytännön ratkaisu, jonka keskeisenä osana on tietoliikenteen salauksen ja todennuksen tekevä Internet Protocol Security -protokolla (IPSec). Käytännön ratkaisusta testataan hallinta-aseman ja reitittimien välistä yhteyttä suojattuna IPSecillä.

Abstract:

Information security has become an important issue during the last years. According to the latest researches, the number of attacks has grown and the attacks are focused more often on routers. In the future quality of service (QoS) will also be important in the network. Security and QoS create new challenges for network management. In this thesis the terms of information security and how security services can be implemented to network management are described. Model and solution for securing network management system are also presented in this thesis. IPSec is explained in theory and used for securing network management connections in the presented solution.

Sisältö

Termejä

3DES	Triple DES. Parannettu versio DES-salausalgoritmista. 3DES:ssa käytetään DES:a kolmeen kertaan kahdella tai kolmella avaimella, joten avainpituus muodostuu kolminkertaiseksi verrattuna DES:iin.
AES	Advanced Encryption Standard. Vuonna 2001 standardoitu symmetrinen salausalgoritmi.
AH	Authentication Header. IPSeciin kuuluva autentikointiprotokolla, joka tarkistaa myös eheyden.
DDoS	Distributed Denial of Service. Hajautettu eli useammalta laitteelta yhtäaikaa tuleva DoS-hyökkäys.
DES	Data Encryption Standard. Symmetrinen salausalgoritmi.
DMZ	Demilitarized Zone. Demilitarisoitu alue. Verkko, joka sisältää julkisia palveluita, on erotettu organisaation sisäisestä verkosta ja johon pääsyä on yleensä rajattu myös julkisen verkon suunnasta.
DOI	Domain Of Interpretation. IPSec DOI (tulkinta-alue) määrittelee eri osien yhteistoiminnan.
DoS	Denial of Service. Palvelunesto. Hyökkäystyyppi, jolla pyritään lamauttamaan jokin palvelu.
ESP	Encapsulation Security Payload. IPSecin salausprotokolla, jolla voidaan myös todentaa paketin alkuperä ja eheys.
FTP	File Transfer Protocol. Yhteydellinen tiedonsiirtoprotokolla.
HMAC	Keyed-hash Message Authentication Code. Mekanismi, jolla voidaan laskea eheys- ja todennussumma. Sen avulla voidaan varmistaa viestin alkuperä ja eheys.
ICMP	Internet Control Message Protocol. TCP/IP-protokollaperheen protokolla vikatilanteiden raportointiin ja ongelmien paikantamiseen.
IDS	Intrusion Detection System. Hyökkäyksen havainnointijärjestelmä.
IETF	Internet Engineering Task Force. Internetin standardeja kehittävä organisaatio.
IKE	Internet Key Exchange. IPSecin automaattinen avainten hallintaprotokolla.
IOS	Internet Operating System. Ciscon kehittämä verkkolaitteiden käyttöjärjestelmä.

IP	Internet Protocol. Verkkokerroksen protokolla TCP/IP-protokollaperheessä.
IPSec	Internet Protocol Security. Internetin IP-tasolla toimiva tietoturva-protokolla.
IPSec-tunneli	IPSec-tunnelilla tarkoitetaan SA-parin muodostamaa yhteyttä IPSec-laitteiden välillä.
IPv4	IP versio 4. Yleisin nykyisin käytetyistä verkkoprotokollista.
IPv6	IP versio 6. IPv4:n seuraaja, jossa useita parannettuja ominaisuuksia.
ISAKMP	Internet Security Association and Key Management Protocol. Malli avainten ja turvallisuussopimusten hallintaan.
ISO	International Standards Organization. Kansainvälinen standardointijärjestö.
ITU	International Telecommunication Union. Kansainvälinen tietoliikennealan yhdistys. Sen sektori ITU-T julkaisee muun muassa suosituksia ja standardeja.
IV	Initialization Vector. Alustusvektori on satunnainen bittijono, jota käytetään samankaltaisuuden hävittämiseen tietoturva-algoritmeissa.
LAN	Local Area Network. Lähiverkko.
MAC	Message Authentication Code. Todennussumma eli sen avulla voidaan varmistaa viestin alkuperä.
MD	Message Digest, eheyssumma, tiiviste. MD:ä käytetään siirtovirheiden havaitsemiseen.
NIDS	Network Intrusion Detection System. Verkosta tulevien hyökkäysten havainnointijärjestelmä.
NIST	National Institute of Standards and Technology. Yhdysvaltalainen virasto, joka huolehtii muun muassa tietoturva-algoritmien standardoinnista.
OSI	Open Systems Interconnection. ISO:n 7-kerroksinen viitemalli tietoliikenteelle.
RFC	Request For Comments. IETF:n julkaisema dokumenttisarja, joka sisältää ohjeita, standardiehdotuksia ja standardeja.
RSA	Rivestin, Shamirin ja Adlemanin kehittämä julkisen avaimen salausalgoritmi.

SA	Security Association, turvayhteys. Pelkällä SA:lla tarkoitetaan yleensä IPSec SA:ta. Kahdella SA:lla määritellään kaksisuuntainen IPSec-yhteys. Jos käytetään sekä AH:ta että ESP:a tarvitaan yhteyteen neljä SA:ta.
SHA	Secure Hash Algorithm. Eräs yleisesti käytetty tiivistefunktio. Nykyisin käytössä versio SHA-1 ja uudemmat.
SKEME	A Versatile Secure Key Exchange Mechanism for Internet. Eräs vaihtoehto IPSecin avaintenhallintaprotokollaksi.
SNMP	Simple Network Management Protocol. SNMP on TCP/IP-protokollaperheen verkonhallintaprotokolla.
SSH	Secure Shell. SSH on TCP/IP:n sovelluskerroksella toimiva tietoturvaprotokolla, jossa on tietoturvaongelmia.
SSH2	Secure Shell versio 2 on uusi parannettu versio SSH:sta.
SSL	Secure Sockets Layer. Netscapen erityisesti HTTP-yhteyksien suojaamiseen kehittämä tietoturvaprotokolla. Viimeinen versio on 3. Katso myös TLS.
S/WAN	Secure Wide Area Network. Turvallinen laajan alueen verkko.
TCP	Transmission Control Protocol. TCP/IP-protokollaperheen kuljetuskerroksen yhteydellinen ja luotettava kuljetusprotokolla.
TLS	Transport Layer Security. SSL:n version kolme pohjalta sen korvaajaksi kehitetty turvallisuusprotokolla. TLS:a kehitetään IETF:ssä.
TMN	Telecommunications Management Network. ITU-T:n suositus telehallintaverkon arkkitehtuurivaatimuksille.
UDP	User Datagram Protocol. TCP/IP-protokollaperheen kuljetuskerroksen yhteydetön ja epäluotettava kuljetusprotokolla.
VPN	Virtual Private Network. Virtuaalinen erillisverkko. Yksityisten verkkojen yhdiste, joka toimii julkisen verkon päällä.
WAN	Wide Area Network. Laajan alueen verkko. Esimerkiksi useampi LAN yhdistettynä toisiinsa.

1 Johdanto

Tietoturva on noussut ajankohtaiseksi aiheeksi viime vuosien aikana lukuisten tietokonevirus- ja matoepidemioiden [58] myötä. Myös kiinteiden internetliittymien lisääntyminen on lisännyt tietoturvan tarvetta verrattuna 80-lukuun, jolloin tietokoneet olivat fyysisesti erossa toisistaan. Tietomurrot ovat lisääntyneet kasvaneen ja yhä osaavamman käyttäjäkunnan sekä automatisoitujen hyökkäysohjelmistojen kehityksen myötä. Verkon runkolaitteetkaan eivät enää säästy hyökkääjiltä. [44]

Uuden tutkimuksen [44] mukaan verkon runkolaitteisiin kohdistuvat hyökkäykset ovat kasvaneet. Hyökkääjät yrittävät ottaa haltuunsa reitittimen ja käyttää sitä verkon tutkimiseen, välityspalvelimena epämääräisille yhteyksille ja lähetyspisteenä palvelunestohyökkäyksille. Nämä seikat nostavat tämän tutkielman aiheen tärkeäksi.

Asiakkaat haluavat laatua verkkoyhteyksiltään. He haluavat, että verkon nopeus taataan ainakin jossain määrin ja että heidän luottamuksellinen liikenne ei joudu muiden käsiin. Verkonhallinnalla on keskeinen osa tässä. Verkonhallintajärjestelmän avulla voidaan muokata asiakkaan verkkoyhteyksien kapasiteettia, asettaa liikennettä tärkeysjärjestykseen ja säätää tietoturvaominaisuuksia. Hallintajärjestelmä huolehtii myös verkon pääsynvalvonnasta ja asiakkaiden mahdollisesta laskuttamisesta. Jyväskylän yliopiston Terabitti-projektissa on kehitetty verkonhallintaohjelmisto, joka käyttää hyökkäyksille altista telnet-protokollaa konfiguroidessaan reitittimiä [45]. Myös Bernin yliopistossa on kehitetty arkkitehtuuria tulevaisuuden verkkojen hallintaan. Mallissa hallintaohjelma voisi käyttää telnet-protokollaa, jos sen turvallisuus olisi kunnossa [17].

Edellisten kaltaisissa ympäristöissä ongelmaksi muodostuu, miten taata verkonhallintajärjestelmän turvallisuus? Miten voidaan taata asiakkaan tietojen luottamuksellisuus? Kuinka todeta, että asiakas on juuri se, joka väittää olevansa? Miten voidaan suojata hallintaliikenne hallinta-asemalta reitittimille? Tässä tutkielmassa vastataan edellisiin kysymyksiin ja esitellään teknologioita, joilla ne pystytään toteuttamaan. Erityisesti verkonhallintaliikenteen tietoturva on tarkastelun alla tässä tutkielmassa.

Ratkaisuna verkonhallintajärjestelmän tietoturvaan on erilaiset käyttäjien ja laitteiden todennusmenetelmät ja tietoliikenteen salaus. Tietoliikenteen suojaus on tehtävä yleisellä standardilla, jotta eri palveluntarjoajien väliset hallintayhteydet voidaan salata myös tulevaisuudessa. Verkosta tulevat hyökkäykset pitää torjua ja niiden varalta on asennettava palomuureja. Lisäksi käyttöjärjestelmät on oltava oikein konfiguroituja. Laitteiden fyysinen suojaus ja varmuuskopioinnit sekä kopioiden oikea säilyttäminen takaa turvallisuuden varkauksien varalta.

Tutkielmassani olen kehittänyt organisaation verkon tietoturvamallin, jonka esittelen luvussa kaksi. Mallin pohjalta voi suunnitella organisaatiolle turvallisen verkon, jossa tarjotaan turvallisesti palveluja sekä sisä- että ulkoverkkoon. Luvun kaksi alussa määrittelen lisäksi tietoturva-käsitteen ja siihen liittyvää termistöä mallia varten.

Luvussa kolme käyn läpi kryptografisia menetelmiä, joita tietoturvaratkaisussani hyödynnetään. Kolmas luku jakaantuu symmetristen salausalgoritmien kuten *Data Encryption Standard* (DES), epäsymmetristen salausalgoritmien kuten *RSA* ja tiivistefunktioiden kuten *Message Digest 5* (MD5) käsittelyyn. Lisäksi käsittelen joitakin hyökkäystyyppejä edellä mainittuja menetelmiä vastaan.

Internet Protokollan (IP) version 4 ja 6 käyn läpi neljännessä luvussa. Lisäksi esittelen siinä verkonhallintajärjestelmien periaatteet. Viidennessä luvussa esittelen *Internet Protocol Security* -protokollan (IPSec), joka on suuressa osassa tässä tutkielmassa esittämässäni tietoturvaratkaisussa.

Kuudennessa luvussa sovellan organisaation verkon tietoturvamallia verkonhallintajärjestelmän suojaamiseen ja analysoin kuinka hyvin uhat on saatu torjuttua. Esitän myös esimerkkiratkaisun verkonhallintajärjestelmän turvaamiseksi käyttäen hyväksi edellisissä luvuissa esitettyjä teknologioita. Vastaavasta aiheesta ei ole aiemmin tieteessä tehty julkaisua, joten tämä on aivan uutta. Teen yhteenvetoa tutkielmasta ja pohdin verkonhallinnan tietoturvan tulevaisuutta luvussa kahdeksan.

Tutkielman lopuksi liitteinä on tietoa tuesta eri protokollille verkkolaitteissa ja kommentoituja esimerkkiasetuksia IPSecin osalta Ciscon reitittimiin ja Linuxin FreeS/WANiin.

2 Verkon tietoturva

Tässä luvussa esitellään tietoturvan perusteet, jotka ovat tarpeen myöhempien lukujen ymmärtämiseksi. Määrittelen muun muassa käsitteet luottamuksellisuus, todennus ja kiistämättömyys, jotka eivät ole ehkä ennestään tuttuja. Lisäksi termit eivät ole aivan vakiintuneet Suomessa ja muualla maailmassa. Tässä tutkielmassa käytetään termejä tämän luvun määrittelyjen mukaan. Käyn myös läpi hyökkäystyyppejä, joilta järjestelmiä suojataan.

2.1 Turvallisuus

Turvallisuus käsitetään yleensä siten, että siihen kuuluu [87]:

- turvallisuusjohtaminen,
- tuotannon ja toiminnan turvallisuus,
- työsuojelu,
- ympäristöturvallisuus,
- pelastustoiminta,
- valmiussuunnittelu,
- tietoturva[1],
- henkilöturvallisuus,
- toimitilaturvallisuus,
- ulkomaantoimintojen turvallisuus ja
- rikosturvallisuus.

Tietoturva on siis osa suurempaa turvallisuuden käsitettä. Nyt käsite turvallisuus on selvempi ja siirrytään tietoturvan määrittelyyn.

[1] Tietoturvasta käytetään myös nimeä tietoturvallisuus.

2.2 Mitä tietoturva on?

Elektroniseen tietoturvaan kuuluu tärkeimpinä tehtävinä luotettava tiedonsiirto ja tiedon varastointi. Tietoturva organisaation ja ylläpitäjän kannalta vaatii organisointia, arviointia ja valintoja turvallisuustuotteiden suhteen. Tuotteet eivät yksinään ratkaise mitään. Organisaation tietoturva määritellään tietoturvapolitiikassa. Tietoturva voidaan jakaa kolmeen osaan [78]:

- Hyökkäys tietoturvaa vastaan: Mikä tahansa toimi, joka vaarantaa organisaation hallitseman tiedon turvallisuuden.
- Turvamekanismi: Mekanismi, joka on suunniteltu hyökkäyksien havaitsemiseen, estämiseen ja toipumiseen.
- Turvapalvelut: Palvelu, joka laajentaa turvallisuutta tiedon käsittelyssä järjestelmien sisällä ja organisaation tiedonsiirrossa. Palvelun on tarkoitus suojella tietoa hyökkäyksiltä. Yhtä tai useampaa turvamekanismia käytetään muodostamaan turvapalvelu.

Nämä osat käydään nyt läpi kääntäen seuraavissa alaluvuissa.

2.3 Turvapalvelut

Mitä turvapalvelut käytännössä ovat? Otetaan esimerkki sähköisestä sopimuksesta. Sähköiset sopimukset eivät saa olla kuin osapuolten nähtävissä. Sopimukset voidaan allekirjoittaa sähköisesti ja siten saada juridinen pitävyys sopimukselle. Sähköisessä muodossa olevalle sopimukselle pystytään varmistamaan ettei kukaan ole muuttanut sopimusta jälkeenpäin. Sopimus on lisäksi aina osapuolten nähtävillä kun he tarvitsevat sitä. Nämä palvelut voidaan määritellä seuraavasti.

Luottamuksellisuus (engl. secrecy)

Tiedot ja järjestelmät ovat käytettävissä vain niille, jotka ovat siihen oikeutettuja. Sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja, eikä muutoin käsitellä tietoja. [83]

Eheys (engl. integrity)

Tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena. [83]

Käytettävyys (engl. usability)[2]

Järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa. Tiedot eivät ole tuhoutuneet tai tuhottavissa vikojen, tapahtumien tai muun toiminnan seurauksena. [83]

Todentaminen (engl. authentication)

Todentaminen (autentikointi) tarkoittaa osapuolten (henkilö tai järjestelmä) luotettavaa tunnistamista. [83]

Kiistämättömyys (engl. non-repudiation)

Kiistämättömyys tarkoittaa tapahtuneen todistamista jälkeenpäin, jolloin tavoitteena on juridinen sitovuus. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. [83]

Pääsynvalvonta (engl. access control)

Pääsynvalvonnalla tarkoitetaan verkkojen tietoturvan yhteydessä kykyä rajoittaa ja kontrolloida pääsyä järjestelmiin. Pääsyn kontrolloimiseksi pitää pystyä ensin todentamaan pyrkijä, jotta valtuudet (käyttöoikeudet) pystytään yhdistämään pyrkijään. [78]

Luotettavan tietoverkon tulisi tarjota käyttäjälleen ainakin luottamuksellisuus, eheys ja käytettävyys. Nämä riippuvat kuitenkin käytetystä tietoturvapolitiikasta. Tietoturvapolitiikka ei ole yksikäsitteinen, vaan se riippuu aina organisaation tiedon arvosta.

[2] Toinen vastaava termi on saatavuus (engl. availability)

Tietoturva

Tietoturvalla tarkoitetaan tietojen, järjestelmien ja palveluiden asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. [83]

Tietoturva käsittää siis myös fyysisen suojaamisen toimenpiteet. Niitä ei kuitenkaan käsitellä tässä tutkielmassa vaan pääpaino on elektronisen tiedon turvallisuudessa.

2.4 Tietoturvamekanismi

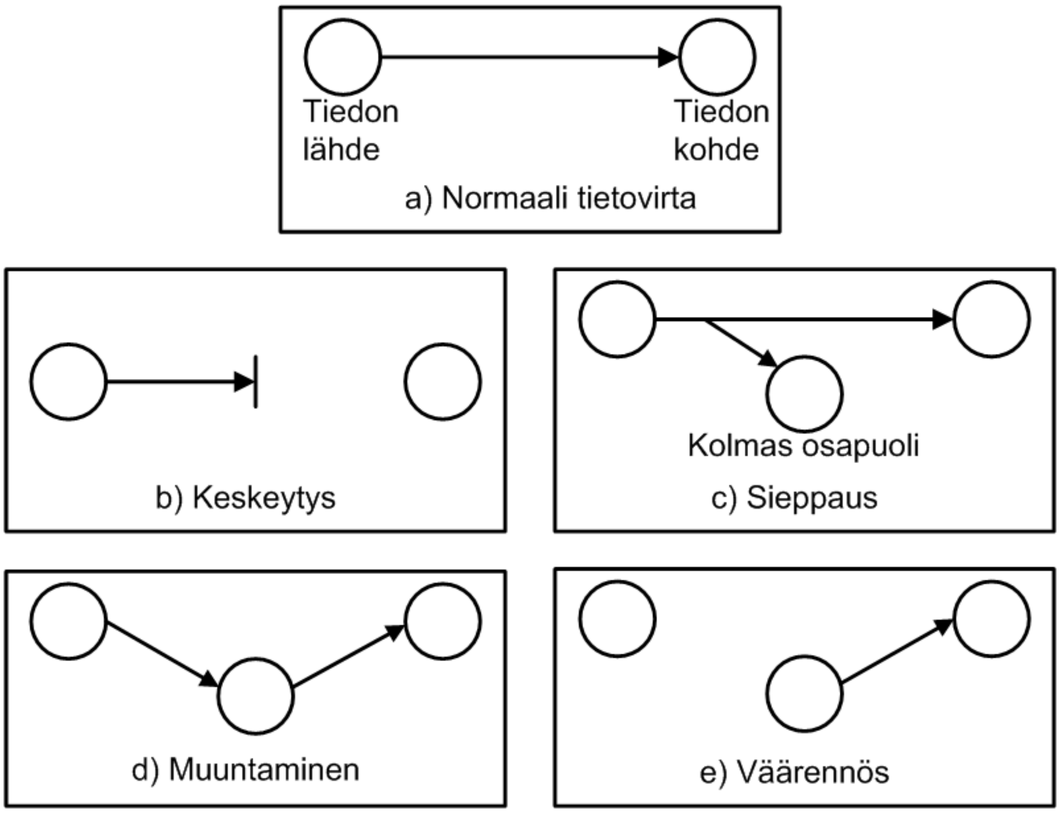
Tietoturvamekanismi on tapa, jolla aiemmin mainittuja palveluja pystytään toteuttamaan. Tämän tutkielman myöhemmissä luvuissa esitetään joitakin mekanismeja, joissa käytetään pääsääntöisesti kryptografisia menetelmiä. Mekanismeista voidaan pitää esimerkkeinä allekirjoitusta ja salakirjoitusta.

2.5 Tietoturvahyökkäys

Tiedonsiirron tavoitteena tietokoneessa tai verkossa on siirtää informaatiota turvallisesti paikasta toiseen. Tietoturvauhat, joilta tietokoneverkko pyritään suojaamaan ovat seuraavanlaisia [47], [78]:

- *Keskeytys* (engl. *interruption*) - Järjestelmän osa tai sen osia on rikkoutunut tai saatettu käyttökelvottomaksi tahallisesti, esimerkiksi yhteys on katkaistu. Tällainen hyökkäys on uhka tiedon käytettävyydelle (saatavuus).
- *Sieppaus* (engl. *interception*) - Luvaton osapuoli (esimerkiksi henkilö tai tietokone) pääsee käsiksi järjestelmän osiin ja pystyy sieppaamaan (luottamuksellisia) tietoja. Tämä on hyökkäys luottamuksellisuutta kohtaan.
- *Muuntaminen* (engl. *modification*) - Luvaton osapuoli pystyy sieppaamisen lisäksi, muuntamaan tietoja tai järjestelmän osia. Tämä on hyökkäys tiedon ja järjestelmän eheyttä vastaan.

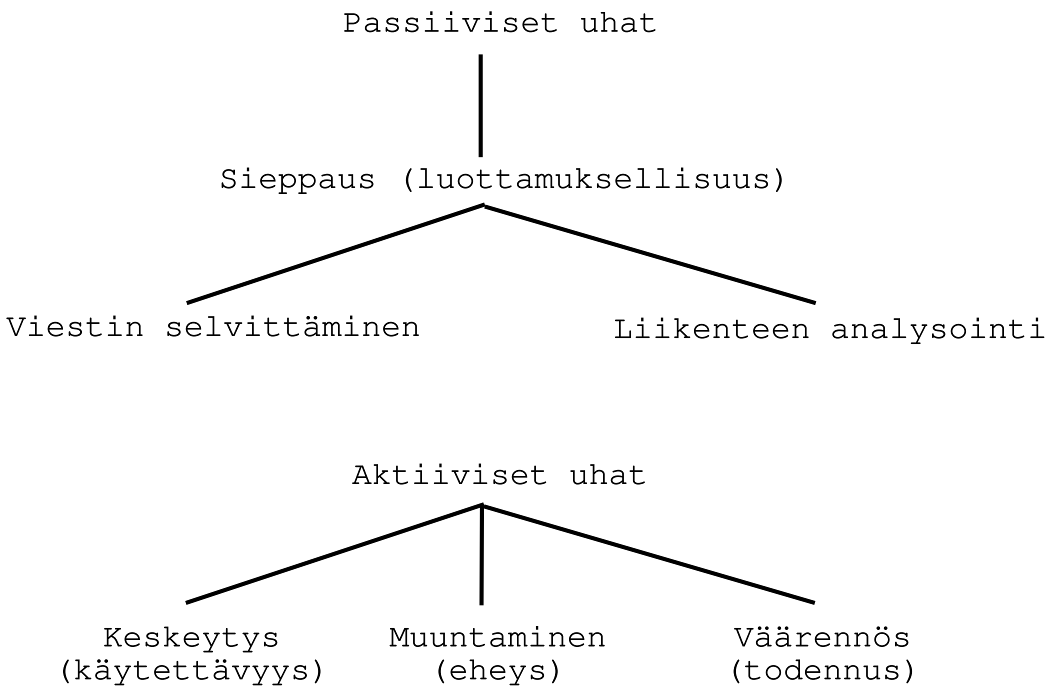
- *Väärennös* (engl. *fabrication*) - Luvaton osapuoli pystyy syöttämään järjestelmään omia tietojaan oikean sijasta. Tämä on myös uhka tiedon eheydelle.



Kuva 2.1: Tietoturvauhat [47],[79]

Kuvassa 2.1 esitetään nämä uhat. Siinä on kuvattu ensin normaali tietovirta ja sen jälkeen eri uhat. Uhkien kohdalla näkyy niiden vaikutus tietovirtaan. Tästä saadaankin nyt toinen tapa jaotella uhkia ja hyökkäyksiä. Se on jakaa ne kahteen ryhmään: aktiivisiin ja passiivisiin. Kuvassa 2.2 esitetään tämä jaottelu.

Passiivisissa hyökkäyksissä tietovirta ei muutu tiedonsiirron osapuolten kannalta mitenkään, joten sitä on vaikea havaita. Salakuuntelu on passiivinen hyökkäys. Siinä pyritään selvittämään liikkuvien viestien sisältö tai tekemään liikenteen analysointia. Analysoinnilla pyritään saamaan selville liikenteen tyyppi, verkon rakenne ja muutakin tietoa organisaatiosta. Muuta tietoa voidaan esimerkiksi päätellä, jos johonkin tiettyyn paikkaan alkaa mennä tavallista enemmän liikennettä. Silloin siellä voidaan olettaa tapahtuvan pian jotain tavallisuudesta poikkeavaa. Passiivisilta



Kuva 2.2: Uhkien jakaantuminen passiivisiin ja aktiivisiin [78]

uhilta voi suojautua käyttämällä vahvaa salausta ja kytkentäistä rakennetta tiedonsiirtoverkossa. Liikenteen analysointia on erittäin vaikea estää, koska lähde- ja kohdeosoitteita on hankala piilottaa ja liikenteen määrää ei ole järkevää pitää tasaisena joka paikkaan kustannussyistä. [78]

Aktiivisissa hyökkäyksissä muunnetaan tietovirtaa kuvan 2.1 kohtien b, d ja e tavoin. Aktiiviset uhat ja hyökkäykset jakautuvat siis kolmeen ryhmään kuvan 2.2 mukaan. [78]

Keskeytys voidaan aiheuttaa esimerkiksi ohjaamalla paketti väärään osoitteeseen tai katkaisemalla fyysinen yhteys. Myös *palvelunestohyökkäyksellä* (engl. *Denial of Service*, DoS) pyritään keskeytykseen. Palvelunestohyökkäys nimeä käytetään yleisesti sellaisista hyökkäyksistä, joissa kohteeseen lähetetään turhia viestejä ja palvelupyyntöjä tukkimaan joko palvelu tai tietoliikennelinja. Näillä pyritään estämään kohteen normaali toiminta. [78]

Muuntaminen on sitä, että tietoa muunnetaan vastaamaan hyökkääjän tarkoitusta. Esimerkiksi muokataan viestiä ”Anna Bertan lukea eilinen viesti” muotoon ”Anna Even lukea eilinen viesti”. Muuntamisen alle voidaan myös lukea viestien viivyttäminen. [78]

Väärentäminen tarkoittaa, että joku teeskentelee olevansa joku toinen. Tällä pyritään saamaan itselle tietoa, joka ei olisi muuten saatavilla. Tämä voi tapahtua esittämällä jokin sellainen palvelupyyntö tai lisäämällä omia oikeuksia järjestelmässä. [78]

Toistohyökkäyksessä (nauhoitushyökkäys) salakuunnellaan ensin viesti ja sen jälkeen lähetetään sitä uudelleen tarvittavan määrän verran. Näin saadaan lähetettyä oikein muotoiltuja viestejä vastaanottajalle, joka vastaa niihin. Vastauksia voidaan analysoida ja sitä kautta purkaa mahdollinen salaus muistakin viesteistä. Tämä hyökkäys koskettaa siis luottamuksellisuutta. Toinen tapa käyttää toistoa on viestien uudelleenlähettäminen niin monta kertaa kuin mahdollista. Tämä on yksi tapa suorittaa DoS-hyökkäys, joka on siis keskeytyshyökkäys. Tämä koskettaa käytettävyyttä. [78], [80]

Aktiivisiakin hyökkäyksiä on vaikea eliminoida kokonaan, koska esimerkiksi DoS-hyökkäyksien pysäyttämiseksi lähes ainoa keino on lisätä vastaanottajan kapasiteettia, mutta myös muita ratkaisumalleja on esitetty. *Probabilistic Packet Marking* (PPM) on yksi malli. Siinä DoS-hyökkäykset estetään verkon toimesta ilman, että vastaanottajan tarvitsee tehdä mitään. Toistohyökkäyksistä analysointia pystytään estämään tiedonsiirtopakettien numeroimisella jolloin jo kerran tai kahdesti saatuihin paketteihin ei enää vastata. [68]

Koska passiivisia ja aktiivisia hyökkäyksiä on vaikea estää, tietoturvamenetelmien tavoitteena onkin suojautua niiltä ennakkoon, pystyä havaitsemaan ne ajoissa ja toipua niiden aiheuttamista ongelmatilanteista. [47]

2.6 Tietoturvan rakentaminen

Tietoturvapolitiikka kuvaa organisaation tietoturvan peruselementit ja luo perustan tietojen turvaamiselle yhtenäisellä tavalla koko organisaatiossa. Turvallisuuspolitiikan luomiseen ei keskitytä tässä tutkielmassa, mutta sen luominen on samankaltainen kuin turvallisuussuunnitelman luomisenkin.

Turvallisuussuunnitelman tekemisen askeleet ovat [35]:

1. Tunnista suojaamisen kohteet.

2. Päättele miltä suojaat niitä.
3. Päättele kuinka todennäköisiä uhat ovat.
4. Tee suunnitelma, jolla voidaan suojella kohteita kustannustehokkaalla tavalla.
5. Arvioi prosessia jatkuvasti uudelleen ja tee tarvittavat muutokset heikkouksia löydettäessä.

Tässä tutkielmassa keskitytään kohtaan neljä lukuun ottamatta kustannusvertailuja.

2.6.1 Common Criteria (CC) - standardi tietoturvan arviointiin

Common Criteria on *International Organization for Standardisation* (ISO) -järjestön standardi 15408. Se määrittelee tietoturvan arvioinnin kriteerit ja integroi Yhdysvalloissa (*Trusted Computer System Evaluation Criteria*, TCSEC ja *Federal Criteria*, FC), Euroopan Unionissa (EU) (*Information Technology Security Evaluation Criteria*, ITSEC) ja Kanadassa (*Canadian Trusted Computer Product Evaluation Criteria*, CTCPEC) kehitetyt arviointikriteeristöt. CC on viralliselta nimeltään *Evaluation Criteria for Information Technology Security*. CC:n dokumentit jakautuvat kolmeen osaan. [22], [84]

Ensimmäisessä osassa on johdanto CC:aan ja yleinen malli. Mallissa määritellään tietoturvallisuuden arvioinnin periaatteet ja esitetään yleinen arviointimalli. [22]

Toisessa osassa käsitellään turvallisuuden toiminnallisia vaatimuksia ja annetaan joukko toiminnallisia komponentteja standardiksi tavaksi kuvata arvioinnin kohteen turvatoimintoja. [22]

Kolmannessa osassa on turvallisuusvakuutuksen vaatimukset. Osassa muodostetaan myös standardi tapa esittää kohteen vakuutusvaatimukset. [22]

CC on melko teoreettinen ja yleiskäyttöinen. Se ei sovellu suoraan käytettäväksi tai verrattavaksi tähän tutkielman aiheeseen, jossa käsitellään verkon tietoturva-asioita.

2.6.2 Passiivinen ja aktiivinen tietoturva

Perinteisesti tietoturva on ollut passiivista ja puolustavaa. Passiivisiin ja puolustaviin tietoturvamekanismeihin luetaan salausmenetelmät ja perinteinen pääsynvalvonta (esimerkiksi suodatuslistat). Nykyään verkot ja järjestelmät ovat kehittyneet ja niissä käytetään passiivisten menetelmien lisäksi aktiivisia menetelmiä. Aktiivisia menetelmiä ovat muun muassa luotettua kolmatta osapuolta käyttävä todennus ja digitaaliset allekirjoitukset. [51]

Seuraavassa alaluvussa esittelen joitakin aktiiviseen ja passiiviseen tietoturvaan liittyviä ohjelmistoja ja laitteita.

2.7 Verkon tietoturvalaitteita ja -ohjelmia

Tietoturvalaitteiden tarve verkoissa on kasvanut Internetin, verkon kautta tulleiden hyökkäysten määrän ja virtuaalisten erillisverkkojen (engl. *Virtual Private Network*, VPN) tarpeen kasvun myötä. Seuraavaksi esittelen tärkeimpiä tietoturvalaiteita tai -ohjelmia.

2.7.1 Palomuuri

Palomuuria käytetään erottamaan verkon osia muusta verkosta eli sen avulla saadaan luotua sisäisiä verkkoja. Palomuuri tekee tämän suorittamalla pääsyn valvontaa. Pääsyä voidaan rajata muun muassa suodattamalla turhaa liikennettä pois suodatuslistoilla. Nykyaikaiset tiloihin perustuvat palomuurit pitävät kirjaa palomuurin läpi menevistä yhteyksistä ja päästävät niiden liikenteen automaattisesti läpi. Palomuureihin on mahdollista tehdä myös kielto- ja pääsylistoja osoitteiden ja liikenteen tyypin mukaan. Palomuuri voi olla laitteisto tai ohjelmistopohjainen ja siihen on usein yhdistetty myös muita toimintoja.

2.7.2 Hyökkäysten havainnointijärjestelmät

Hyökkäysten havainnointijärjestelmät (engl. *Intrusion Detection System*, IDS) ovat apuna hyökkäysten havainnoinnissa ja mahdollisesti suorittavat aktiivista hyökkäystentorjuntaa. Verkkoliikennettä tarkkailevaa järjestelmää kutsutaan engl. termillä *Network Intrusion Detection System* (NIDS). Tunkeilijoiden havainnointiin ja heikkouksien etsimiseen on kehitetty erilaisia ohjelmia. Linuxille on kehitetty *Linux Intrusion Detection System* (LIDS) [55], joka on vapaasti saatavilla ja on kehitetty laajentamaan kernelin turvallisuutta. Muita ohjelmia on esimerkiksi Tiger heikkouksien etsimiseen, Logcheck lokien tarkkailuun, Snort verkkoliikenteen tarkkailuun ja Tripwire tiedostoissa tapahtuvien muutoksien havainnointiin. [63], [76], [23]

Hyökkäysten havainnointijärjestelmien huono puoli on niiden vaikea konfigurointi ja niiden aiheuttamat useat väärät hälytykset. IDS:n ylläpito vaatii jatkuvaa työtä eikä se ole helppoa. IDS:ä ei kannata ottaa käyttöön organisaatiossa ellei siihen ole varaa panostaa, koska huonosti ylläpidettynä siitä ei ole hyötyä. [3]

2.7.3 Torjuntaohjelmat

Virukset ja madot ovat yleisiä varsinkin Microsoftin Windows-käyttöjärjestelmäympäristössä. Tämä on luonut suuren tarpeen virustorjuntaohjelmistoille, jotka pystyvät havaitsemaan erilaisia haitallisia ohjelmia sekä kiintolevyltä että käyttömuistista. Reitittimien käyttöjärjestelmät ovat toistaiseksi säästyneet virus ja matoepidemioilta, joten tässä tutkielmassa ei kerrota enempää haitallisista viruksista ja madoista. [58], [1]

2.8 Verkon tietoturva

Toimiva verkko vaatii toisaalta laitteiden ja ohjelmistojen helppokäyttöisyyttä ja toisaalta luotettavaa tietoturvaa. Kunnollisen tietoturvan puutetta verkon runkolaitteissa ja hallinnassa voidaan pitää ongelmana. Monet käyttävät vielä nykyään suojaamatonta telnet-yhteyttä reitittimien hallintaan. Kannattavan kaupan harjoittaminen verkkoyhteyksillä puolestaan vaatii luotettavan nopeasti mukautuvan verkon sekä luotettavan ja helppokäyttöisen laskutus- tai verkkomaksujärjestelmän. Reitittimiin on vaikea lisätä omia tietoturvaohjelmistoja, koska reitittimien käyttöjärjestelmät ovat yleensä valmistajakohtaisia, suljettuja ja niiden suorittimet ovat lisäksi usein erityisvalmisteisia.

2.8.1 Verkon tietoturvamalleja

Lähteessä [78] on esitetty yleinen malli verkkoturvallisuudelle. Mallin osat ovat kommunikoinnin osapuolet (jakavat keskenään salaista tietoa), luotettu kolmas osapuoli (salaisen tiedon turvallisena välittäjänä), tiedonvälityskanava ja turvallisuusmekanismi (muuntaa välitettävän tiedon salaisen tiedon avulla siirtokelpoiseen muotoon).

Tämän yleisen mallin mukaan kyseisen palvelun suunnittelussa on neljä pääkohtaa [78]:

1. Turvallisuusmekanismin suunnittelu tiedon muuntamisesta siirrettävään, luottamuksellisuuden säilyttävään, muotoon.
2. Salaisen tiedon luonti, jotta edellä mainittua mekanismia voitaisiin käyttää.
3. Menetelmän kehittäminen salaisen tiedon jakeluun.
4. Protokollan määrittely osapuolten käyttöön. Protokollan avulla määritellään turvallisuusmekanismien käyttö siten, että saavutetaan haluttu palvelu.

Seuraavaksi lähden kehittämään organisaation verkon tietoturvamallia.

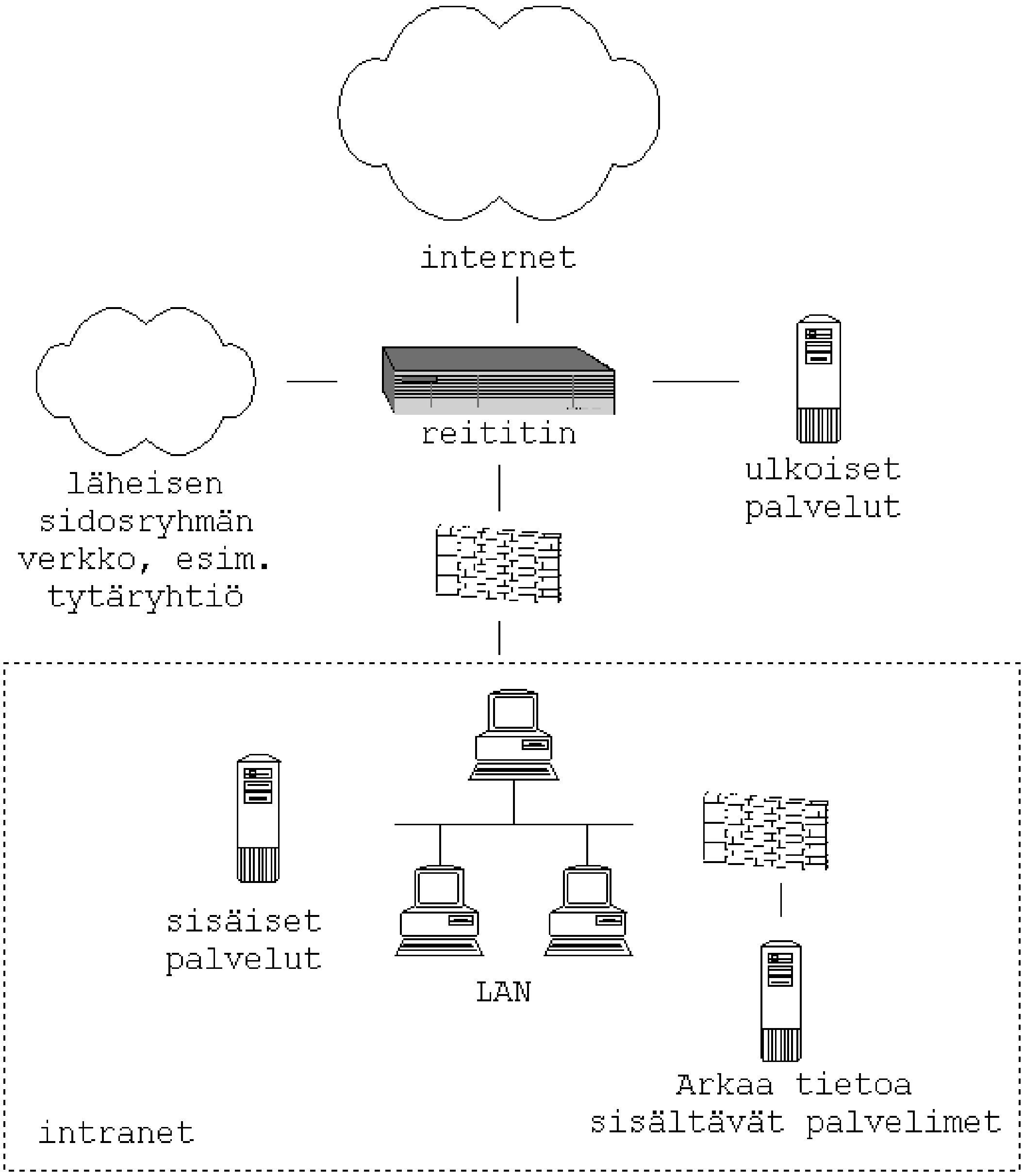
2.9 Organisaation verkon tietoturvamalli

Lähteessä [51] on esitetty verkkojen, elektronisen kaupankäynnin ja yrityksen tietoturvamalli. Muita esimerkkejä on annettu lähteissä [14], [23], [62] ja [34]. Esittelen seuraavassa alaluvussa joitakin näistä.

2.9.1 Kirjallisuudessa esitettyjä malleja

Nikanderin malli

Kuvassa 2.3 on esitetty yrityksen liittyminen julkiseen verkkoon. Julkisen verkon ja sisäisen verkon erottaa toisistaan palomuuri, joka suodattaa pois kaiken tarpeettoman sisääntulevan liikenteen. Liityntäreitittimeen on puolestaan yhdistetty suoraan yrityksen julkiset palvelut ja yhteydet läheisiin sidosryhmiin. Julkisten palveluiden sijoittaminen näin avoimesti on huonoa Nikanderin mallissa, koska palvelut jäävät hyvin alttiiksi palvelunestohyökkäyksille. Intranetissä arkaluontoiset palvelimet ovat sijoitettuna oman sisäisen palomuurin taakse. Sisäiset palvelut on mallissa sijoitettu työaseman tavoin, mutta ne olisi hyvä suojata arkaluotoisen materiaalin tavoin väärinkäytösten varalta. [62]

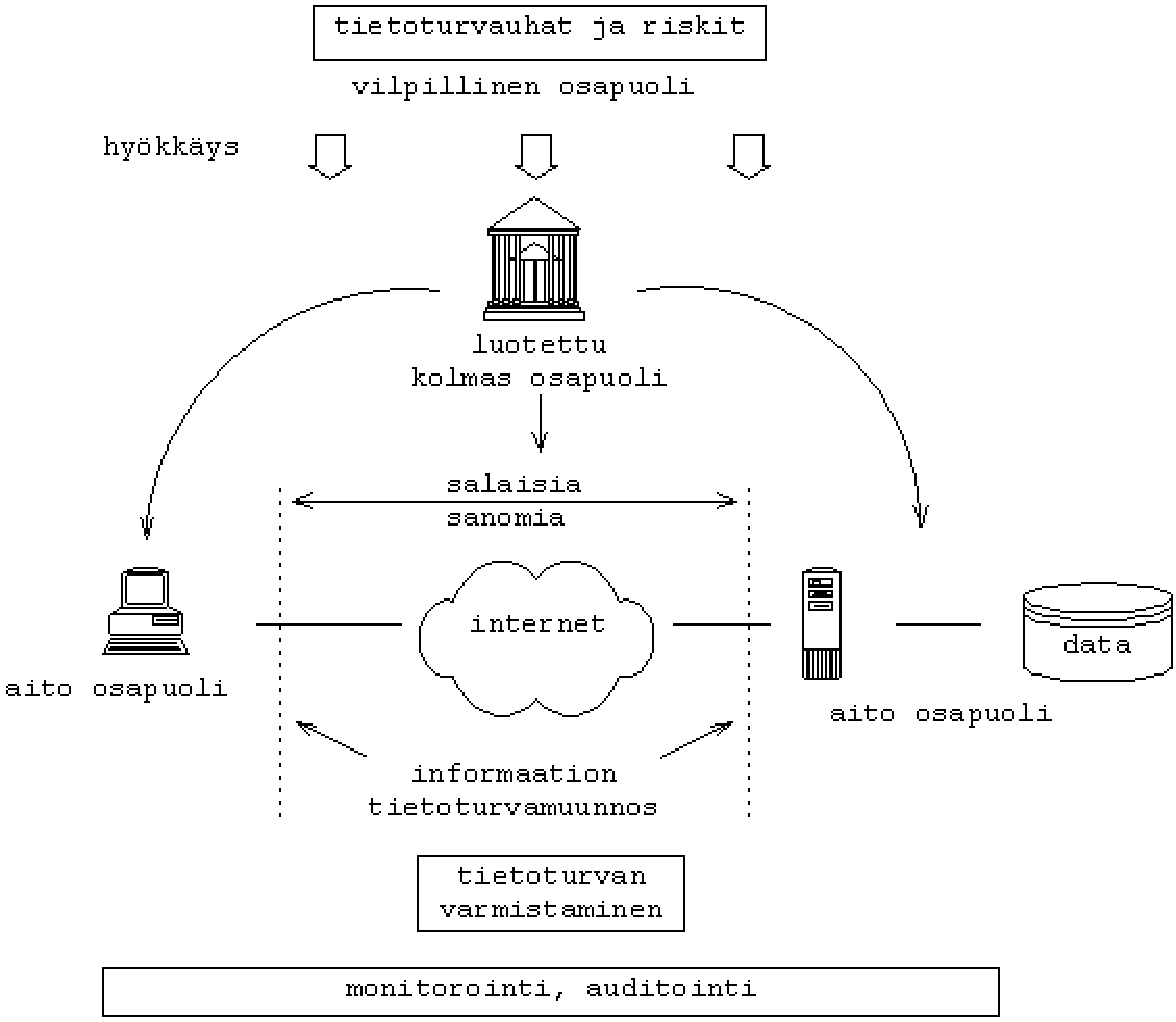


Kuva 2.3: Nikanderin tietoturvamalli [62]

Kerttulan malli

Kerttulan malli rakentuu vähitellen. Ensin esitellään yleinen malli ja sen jälkeen elektronisen kaupankäynnin ja yrityksen mallit.

Lähteessä [51] on esitetty kuvan 2.4 kaltainen yleinen malli passiiviselle tietoturvalle. Malli on hyvin karkea, mutta antaa pohjaa seuraaville malleille. Malli on hyvin samankaltainen kuin alaluvussa 2.8.1 esitetty ratkaisu. Siinä on luotettu kolmas osapuoli, joka auttaa kommunikoinnin osapuolia muodostamaan turvallisen yhteyden, ja vilpillinen osapuoli, joka yrittää saada pahaa aikaan.



Kuva 2.4: Kerttulan malli yleiselle verkkoturvallisuudelle [51]

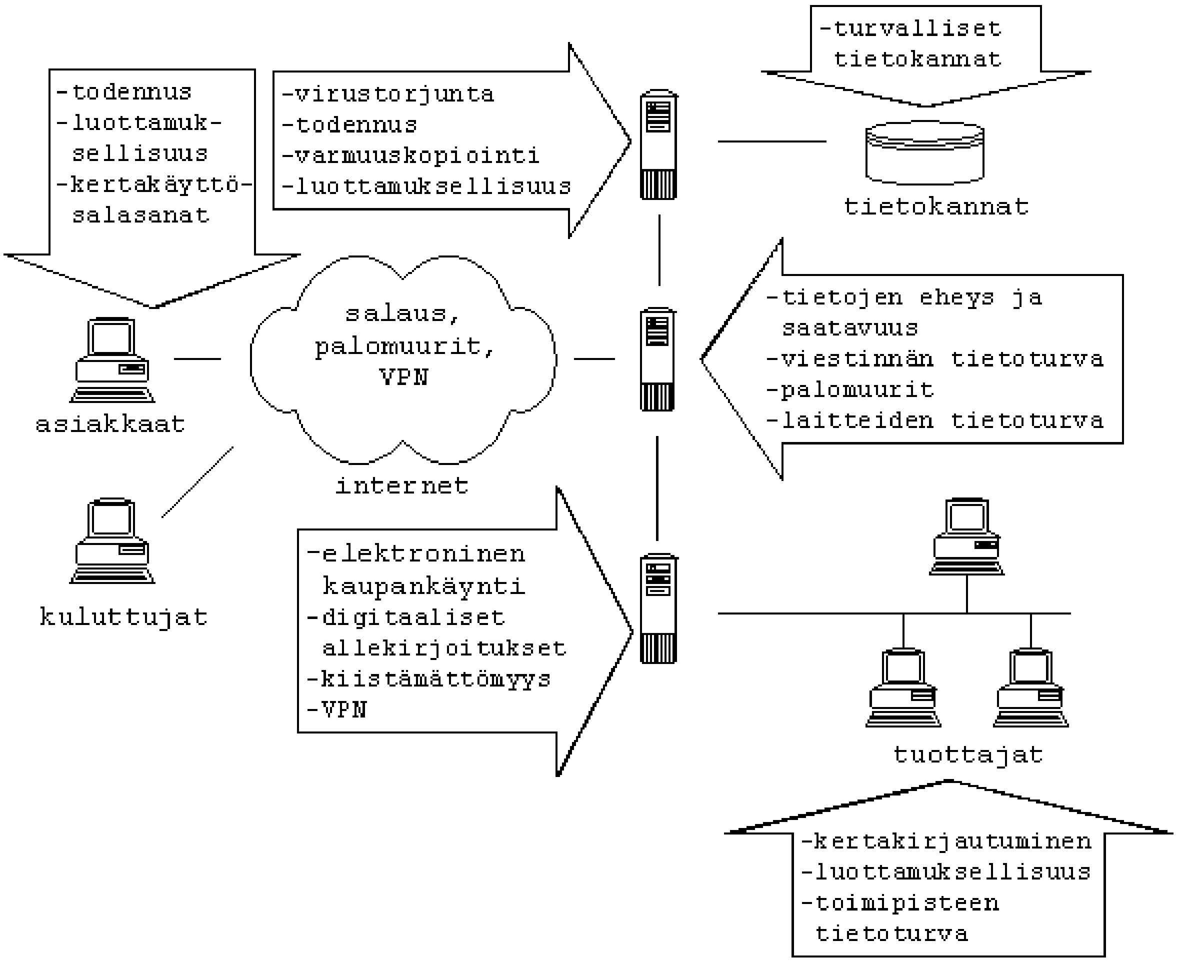
Elektronisen kaupankäynnin mallissa todetaan, että siinä käytetään samoja komponentteja kuin edellisessäkin. Tämä tapaus on kuitenkin monimutkaisempi ja alttiimpi siten hyökkäyksille. Elektronisessa kaupankäynnissä tietoturva on aktiivisempaa. Siinä käytetään monenlaisia tietoturvaprotokollia ja menetelmiä [51]:

- digitaaliset allekirjoitukset,
- kohteen todentaminen,
- sanoman todentaminen,
- avainten jakelu ja hallinta,
- verkkomaksaminen,
- salaisen avaimen järjestelmät,
- julkisen avaimen järjestelmät,
- nollatietotodistukset.

Yrityksen tietoturvamalli esitetään kuvassa 2.5. Siinä on esitetty keinoja, joilla verkko voidaan suojata. Ratkaisu verkon jakamiseen osiin palomuureilla. Osia ovat internet, *demilitarisoitu alue* (engl. *Demilitarized Zone*, DMZ) ja varsinainen intranet. Ratkaisun turvallisuus perustuu sisäverkon ja sen ulkopuolisen liikenteen salaukseen, todennukseen, liikenteen suodattamiseen, turvallisiin käyttöjärjestelmiin, virustorjuntaan ja varmuuskopiointiin. Tämän Kerttulan mallin ongelman on yrityksen sisäverkon tietoturvan puutteellisuus ja luettelomaisuus. Mallissa ei puututa esimerkiksi palomuurien sijaintiin. Lisäksi siinä puhutaan turvallisista tietokannoista, mutta ei esimerkiksi esitetä tietokantapalvelimen suojaamista palomuurilla. [51]

Ciscon SAFE-arkkitehtuuri

SAFE on malli turvallisen verkon suunnitteluun ja toteutukseen. Se perustuu verkon jakamiseen osiin käyttötarkoituksen ja sijainnin mukaan. SAFEssa käytetään kytkentäistä rakennetta vaikeuttamaan verkon kuuntelua. Verkonhallinta on irrotettu omaksi kokonaisuudekseen SAFE-arkkitehtuurissa omalla kaapeloinnillaan tai salatuilla yhteyksillä. SAFE on suunniteltu pääasiassa suurten yritysten verkkoratkaisuksi, mutta skaalautuu myös pienempien verkkojen malliksi vähentämällä osien määrää. Malli soveltuu kuitenkin paremmin suurten organisaatioiden tarpeeseen, koska poistettavien osien päättely ei ole kovin helppoa. Mallissa ei puututa yksittäisten laitteiden kuten reitittimien tai palomuurien tietoturvaan tarkemmin



Kuva 2.5: Kerttulan malli yrityksen tietoturvalle [51]

vaan ne jätetään mallin ulkopuolelle. SAFEn dokumentaatiossa kerrotaan, mitä uhkia kohdistuu eri osioihin ja miten niiltä suojaudutaan yleisellä tasolla. [23]

Seuraavassa alaluvussa esitän oman ratkaisuni organisaation verkon tietoturvamalliksi, koska olen havainnut puutteita edellisissä malleissa.

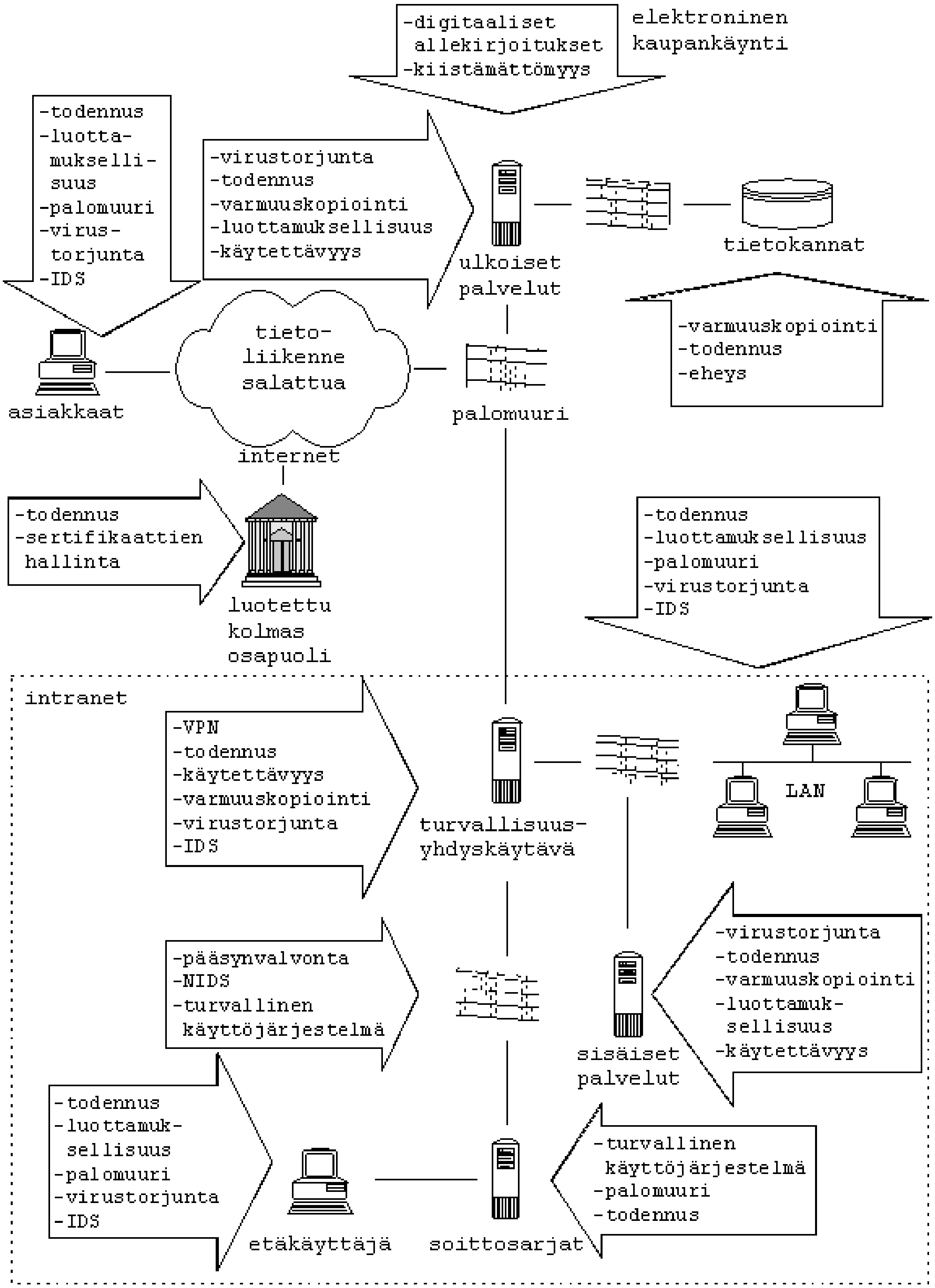
2.9.2 Organisaation verkon tietoturvamalli

Edellisessä alaluvussa esitellyt ratkaisut ovat olleet pohjana kuvassa 2.6 olevalle organisaatioiden verkkojen tietoturvamallille, jonka olen kehittänyt.

Asiakkaan, etäkäyttäjän tai organisaation lähiverkon koneiden turvallisuudesta on huolehdittava ensimmäisenä. Näillä yksittäisillä koneilla on huolehdittava pääsynvalvonnasta hyvillä salasanoilla ja työasemakohtaisilla ohjelmistopalomuureilla. Virustorjuntaohjelmat täytyy pitää päällä koko ajan haitallisten ohjelmien varalta. Lähiverkon koneilla voi lisäturvaa olla tuomassa IDS tai sen sensori keskitetyssä järjestelmässä. Lähiverkossa käytetään kytkentäistä rakennetta, jota painotetaan SAFE-arkkitehtuurissa, estämään salakuuntelu.

Kaikki tietoliikenneyhteydet etäkäyttäjältä tai asiakkaalta salataan salakuuntelun varalta ja liikenne todennetaan muutoksien varalta. Osapuolet todennetaan sertifikaateilla ja/tai salasanoilla, koska muuten salauksella ja liikenteen todennuksella ei ole merkitystä. Sertifikaattien jakoon ja varmistukseen voidaan käyttää luotetun kolmannen osapuolen palvelinta. Turvallisuusyhdyskäytävä hoitaa kaiken organisaation lähiverkkoon tulevan liikenteen salauksen ja purkamisen. Siinä todennetaan myös samalla etäkäyttäjät.

Organisaation sisäverkko (intranet) on erotettu kuvassa 2.6 katkoviivalla. Intranet on pelkästään yrityksen omaan käyttöön tarkoitettu verkko. Rajoitetusti sitä voi mahdollisesti käyttää jotkin yhteistyökumppanit, mutta siitä muodostuu aina tietoturvariski. Organisaation sisäverkkoon tuleva ja sieltä lähtevä liikenne suodatetaan palomuureilla, jotta hyökkääjät eivät pääse yrityksen verkkoon tai pysty lähettämään sieltä tietoa itselleen, jos tunkeutuminen on jo onnistunut. Vain tarpeellinen liikenne kustakin osoitealueesta päästetään läpi. Poikkeukset laitetaan erikseen, jos on tarvetta. Ulkoapäin tultaessa organisaation verkkoon ensimmäisissä laitteissa on oltava turvallinen käyttöjärjestelmä. Erityisesti tällaisia laitteita ovat palomuurit, turvallisuusyhdyskäytävä ja soittosarjoja hoitavat koneet.



Kuva 2.6: Organisaation verkon tietoturvamalli

Sisäisillä palveluilla kuvassa 2.6 tarkoitetaan tietokantapalvelimia, tiedostopalvelimia ja sisäistä WWW-palvelua. Nämä palvelut on eristetty *lähiverkosta* (engl. *Local Area Network*, LAN) palomuurilla ja niille sallitaan vain tarvittava liikenne. Tämä on kuten arkaa tietoa sisältävien palvelimien eristäminen Nikanderin mallissa.

Ulkoiset palvelut eristetään muusta organisaation verkosta hallinnan ja liikenteen tarkkailun helpottamiseksi. Ulkoisia palveluja käytetään myös palomuurin läpi, jotta ylimääräinen liikenne saadaan suodatettua pois kuormittamasta varsinaisia palveluja. Ulkoisten palvelujen tietokannat suojataan vielä erillisellä palomuurilla, koska niissä on yleensä nopeasti muuttuvat kriittiset tiedot. Nyt tietokannat pysyvät vielä kunnossa, vaikka ulkoisia palveluja pystyttäisiin kaappaamaan tai muokkaamaan. Ulkoisia palveluja tuottavilla palvelimilla on käyttöjärjestelmän turvallisuutta lisääviä ohjelmia, jotka rajoittavat palveluja tarjoavien ohjelmien oikeuksia vain tarvittaviin. Elektroninen kaupankäynti tuo omat lisänsä tietoturvapalvelujen vaatimuksiin. Tehdyt kaupat on pystyttävä todistamaan jälkeenpäin (kiistämättömyys). Tämän vuoksi tilaukset allekirjoitetaan digitaalisesti.

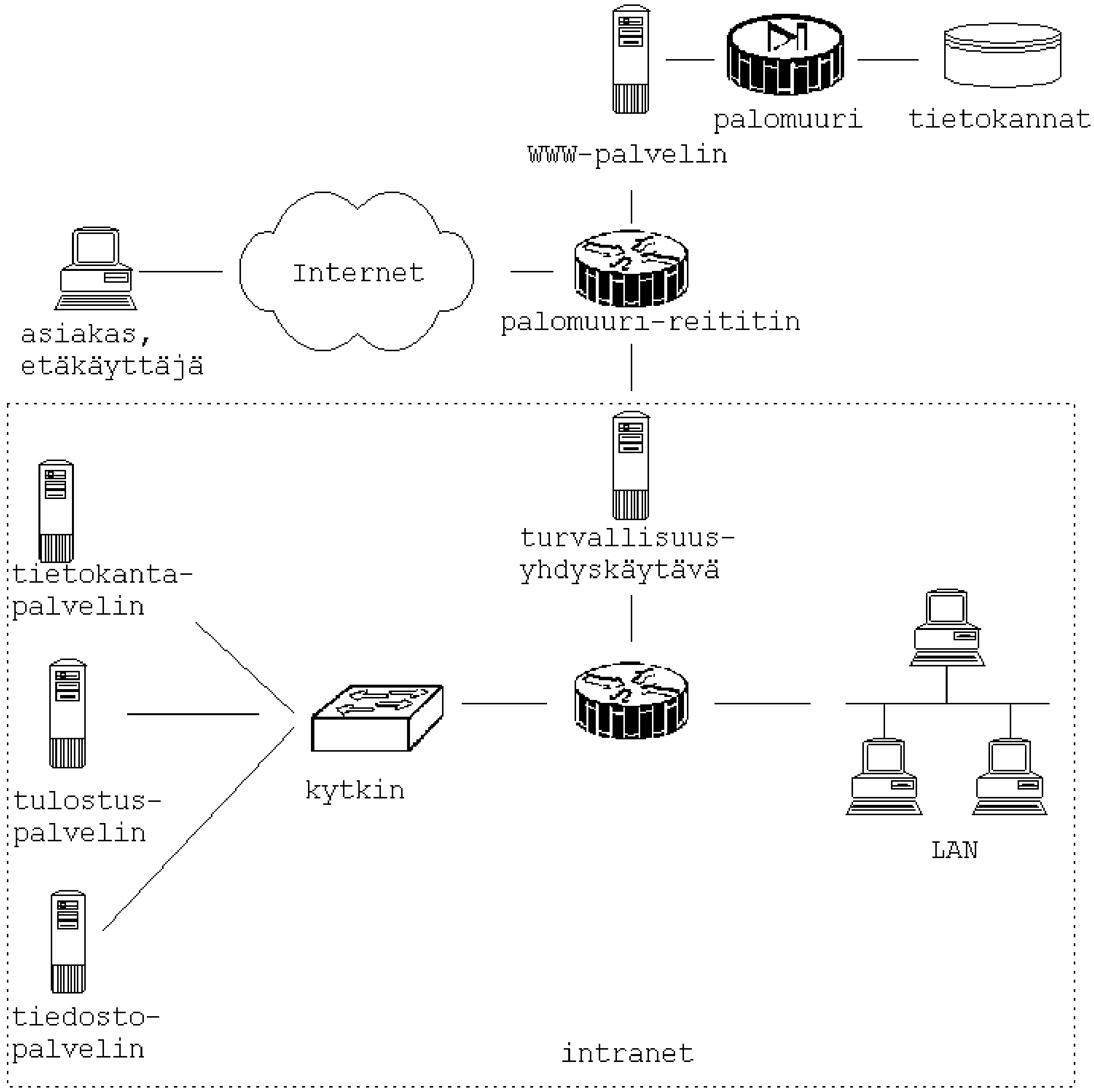
Malli ei pyri olemaan aivan täydellinen, koska aihe on niin laaja. Tarkempi käsittely edellyttää osiin jakamista esimerkiksi seuraavasti: asiakas, luotettu kolmas osapuoli, internet, organisaation julkiset palvelut, organisaation sisäiset palvelut ja LAN.

2.9.3 Esimerkkitoteutus organisaation verkon tietoturvamallista

Kuvassa 2.7 on malliesimerkki verkosta, joka noudattaa edellisessä alaluvussa kehittelemääni organisaation verkon tietoturvamallia. Esimerkkiverkko tarjoaa ulkoisena palveluna WWW:n asiakkaille ja organisaation sisälle tietokanta-, tulostus- ja tiedostopalvelua. Lisäksi turvallisuusyhdyskäytävä mahdollistaa organisaation sisäverkon etäkäytön. Nämä kaikki tehdään mallin mukaan turvallisuudesta tinkimättä.

2.9.4 Tietoturvamallien vertailua

Mainitsin edellisissä tietoturvamalleja esitellessäni joitakin puutteita niistä: Nikanderin mallissa on puutteellinen ulkoisten palvelujen suojaus, Kerttulan yrityksen tietoturvamallissa oli unohdettu sisäiset riskit, SAFE on kehitetty oikein ison verkon tietoturvaan ja on monimutkainen. Omassa mallissani olen ottanut huomioon



Kuva 2.7: Esimerkki organisaation verkosta

muiden mallien puutteet ja todennut ettei siinä ole vastaavia. Kerttulan ja Nikanderin mallit ovat osittain vanhentuneita eikä niissä esimerkiksi mainita SAFEssa painotettua kytkentäistä rakennetta, joka on erittäin hyvä estämään salakuuntelua lähiverkossa.

SAFEssa on hyvää verkonhallinnan tietoturvaan panostaminen ja siinä hallintaliikenne salataan kuten omassa mallissani. Toisena vaihtoehtona SAFEssa esitetään omaa kaapelointia hallintayhteyksille, mutta mielestäni se on liian kallista ja lisäksi turvatonta pelkästään tehtynä. Yhteydet pitää kuitenkin salata fyysisten murtojen varalta.

Kerttulan malli yrityksen tietoturvalle pitää sisällään paljon asiaa luetteloissa, joka ei ole ehkä kaikkein selkein tapa esittää asioita. Mallissani on sama ongelma, mutta asian esittäminen tiivistetysti vaatii sitä. Luettelot ovat molemmissa malleissa asioita, joita täytyy muistaa kyseisissä kohdissa.

Mallissani ei ole otettu huomioon laajan sisäverkon toimintaa, mutta kuvassa 2.6 esitetyt palomuurilla eristetyt sisäiset palvelut ja LAN voisivat kuvata yhtä osastoa. Toiset osastot olisivat vastaavasti yhteydessä turvallisuusyhdyskäytävään.

3 Kryptografiset menetelmät

Tässä luvussa kerron tietoturvan toteuttamiseen tarvittavista kryptografisista menetelmistä. Näitä menetelmiä ovat erilaiset salausmenetelmät ja tiivistefunktiot. Salausmenetelmiä käytetään tiedon luottamuksellisuuden takaamiseen ja tiivistefunktioita tiedon eheyden tarkistukseen. Näiden menetelmien perusteella pystytään myös todentamaan tiedon alkuperä. Tässä tutkielmassa ei esitetä vaativaan matematiikkaan perustuvien salausalgoritmien tai tiivistefunktioiden toimintaa matemaattisella tasolla.

Salaisen avaimen menetelmät voidaan jakaa yleisellä tasolla kahteen rakenteensa perusteella: *tietovirta-* ja *lohkosalaajat*. [78]

Tietovirtasalaaja

Tietovirtasalaaja (jonosalaaja) salaa tietovirtaa bitti tai tavu kerrallaan. Nämä ovat vanhimpia menetelmiä. Esimerkkinä tietovirtasalaajasta on Vigenere. Myös lohkosalaajia voidaan käyttää tietovirtasalaajan tavoin tietyissä moodeissa. [78], [51]

Lohkosalaaja

Lohkosalaajissa algoritmeille syötetään useampi bitti tai merkki kerrallaan eli lohkoina. Yleensä nämä lohkot ovat 64 tai 128 bitin kokoisia. Salaus tapahtuu siis lohko kerrallaan. Jos salattavan tiedon pituus on pienempi kuin lohkon pituus, lisätään tiedon perään täytettä. [51]

3.1 Symmetrinen salaus

Symmetrinen salaus on niin sanottua perinteistä salausta. Symmetrisessä salauksessa osapuolet jakavat saman salaisen avaimen keskenään. Tätä samaa avainta käytetään sekä salaamiseen että purkamiseen. Symmetrinen salaus takaa tiedon luottamuksellisuuden kunhan salainen avain on vain osapuolten hallussa. Symmetrisen salauksen tarjoamasta mahdollisuudesta viestin todennukseen kerrotaan alaluvussa 3.4.1.

3.1.1 Data Encryption Standard (DES) ja Triple DES (3DES)

DES ja sen johdannainen 3DES ovat vielä tällä hetkellä yleisesti käytössä olevia algoritmeja. DES on julkaistu vuonna 1977 yhdysvaltalaisen *National Bureau of Standardsin* toimesta standardikoodilla FIPS PUB 46. Nykyisin virasto tunnetaan nimellä *National Institute of Standards and Technology* (NIST). [24], [78]

DES:ssa tieto salataan 64 bitin lohkoissa. Salausavaimen pituus on 56 bittiä ja sen perään lisätään 8 tarkistusbittiä. DES on salausavaimen pituutensa vuoksi vanhentunut ja se onkin jo murrettu muutamaan otteeseen laskentakapasiteetin avulla. DES:ssa määritellään algoritmin käyttö neljässä moodissa, jotka ovat *Electronic Codebook* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB) ja *Output Feedback* (OFB). Moodeja kuvataan tarkemmin lähteessä [26]. [78], [51], [24]

3DES:ssa voidaan käyttää kahta tai kolmea 56 bitin salausavainta, joten sen salausavaimien yhteenlasketun pituuden voi laskea vastaavan 112-168 bittistä yksittäistä avainta. 3DES:a voidaan käyttää eri tavoin. Salaamalla viesti kolmeen kertaan käyttäen joka kerta eri avainta (DES-EEE3, missä E=encrypt[3]) tai salaus-purku-salaus -operaatiolla (DES-EDE3, missä E=encrypt ja D=decrypt[4]), jossa käytetään myös kolmea eri avainta. Kahdella avaimella 3DES:a käytetään samoin kuin kolmella avaimella, mutta ensimmäisellä ja kolmannella kerralla käytetään samaa avainta (DES-EEE2 ja DES-EDE2). American National Standards Instituten (ANSI) standardissa X9.52 määritellään seitsemän 3DES:n käyttömoodia, joita ei tässä käsitellä. [51], [24]

DES on pikkuhiljaa poistuva standardi ja 3DES:kin on pikkuhiljaa korvautumassa uudella standardilla, jota esittelen seuraavassa alaluvussa. DES:a ja 3DES:a on jo käsitelty aiemmin riittämiin kirjallisuudessa [78], [51] ja [59], joten en tässä käy niitä tarkemmin läpi.

3.1.2 Advanced Encryption Standard (AES)

AES on yhdysvaltalaisen viraston, NIST:n, vuonna 2001 julkaisema standardi DES:n seuraajaksi käytettäväksi sähköisen tiedon salauksessa. AES:n algoritmiksi valittiin Rijndael-algoritmi pitkän valintaprosessin päätteeksi. AES määrittelee Rijndaelin

[3] encrypt on suomeksi salaus.
[4] decrypt on suomeksi salauksen purku.

käytön 128, 192 ja 256 bitin avainpituuksilla. AES:ssa tämän symmetrisen lohkosalaajan lohkon kooksi määritellään 128 bittiä. Näin määriteltyä Rijndael-algoritmia kutsutaan AES-algoritmiksi. Rijndael tukee myös muita lohkokokoja ja avainpituuksia, mutta niitä ei ole otettu mukaan AES:iin. [5]

AES:a voidaan käyttää eri avainpituuksilla, joten niille on annettu nimet AES-128, AES-192 ja AES-256 avainpituuden mukaan. Taulukossa 3.1 on esitetty AES:n eri avain-lohko-kierros -yhdistelmät. Standardin mukaisen toteutuksen pitää toteuttaa AES vähintään yhdellä yllä mainituista avainpituuksista. Heikkoja tai puoliheikkoja avaimia ei AES:lle ole löydetty. [5]

Nimi	Avaimen pituus bitteinä	Lohkon koko bitteinä	Kierrosten lukumäärä
AES-128	128	128	10
AES-196	196	128	12
AES-256	256	128	14

Taulukko 3.1: AES:n avain-lohko-kierros -vertailu [5]

AES:a saa käyttää vapaasti ja monet sovellukset [39], [61], [73] tukevatkin jo sitä. AES on analysoitu usean vuoden valintaprosessin aikana hyvin ja siitä ei ole löydetty heikkouksia [15]. AES on myös nopeampi [72], [11] kuin 3DES vastaavalla avainpituudella, joka suosii AES:n käyttöön siirtymistä. AES:n matemaattinen puoli on esitetty tarkasti lähteessä [5].

3.1.3 Yhteenveto symmetrisestä salauksesta

Symmetrisiä salausalgoritmeja on kehitetty paljon ja tässä käsiteltiinkin vain myöhemmin tutkielmassa esitettäviin tietoturvaratkaisuihin liittyviä algoritmeja. Eri salausalgoritmien vahvuuksia on hankala vertailla, koska peruslähtökohtana algoritmeilla on se, että niiden murtamiseen ei ole muuta keinoa kuin laskentakapasiteetti. Tämä merkitsee sitä, että vertailua voidaan yleensä suorittaa avainpituuksien perusteella. Mitä pidempi avain, sitä parempi ja pidempiaikainen turva.

Mikään salausalgoritmi nykyisin käytetyillä avainpituuksilla ei luultavasti ole turvallinen enää monien kymmenien vuosien päästä, koska tietokoneiden kehitys menee huimaa vauhtia eteenpäin. Tämä on syytä muistaa suunniteltaessa salauksen käyttöä eli on syytä käyttää aina hieman suurempaa avainpituutta kuin luulee tarvitsevansa.

3.2 Epäsymmetrinen salaus

Epäsymmetrisessä salauksessa käytetään kahta salausavainta. Julkinen avain on kaikkien käytössä ja salainen avain henkilökohtainen. Epäsymmetristä salausta kutsutaan myös julkisen avaimen salaukseksi. Siitä on johdettu menetelmä, digitaalinen allekirjoitus, käyttäjän luotettavaan tunnistukseen. Digitaalisessa allekirjoituksessa lähettäjä pystytään toteamaan myös ulkopuolisen toimesta jälkeenpäin ja näin saavuttamaan kiistämättömyys. Tässä tutkielmassa ei kuitenkaan käsitellä digitaalista allekirjoitusta enempää. Osa julkisten avainten menetelmistä soveltuu käytettäväksi myös salaisten avainten vaihdossa. [78], [47]

Yleensä menetelmää käytetään siten, että julkinen avain on tiedon salaamista varten ja salaista avainta käytetään purkamiseen. Tämä toteuttaa kuitenkin vain luottamuksellisuuden. Viestin todennus, josta kerron lisää alaluvussa 3.4, jää toteutumatta. [78], [47]

Toinen tapa käyttää epäsymmetristä salausta on salaaminen lähettäjän salaisella avaimella ja purkaminen lähettäjän julkisella avaimella, jolloin viestin todennus voidaan tehdä.

Jotta epäsymmetrisellä salauksella saataisiin toteutettua sekä todennus että luottamuksellisuus, on viesti salattava kahteen kertaan. Ensin viesti salataan lähettäjän salaisella avaimella jolloin todennus toteutuu ja sitten vastaanottajan julkisella avaimella luottamuksellisuuden takaamiseksi.

Julkisen avaimen salaus on keksitty vasta 1976 ja sen jälkeen on esitetty useita eri menetelmiä. Vain kolme on kuitenkin todettu luotettaviksi ja tehokkaiksi. Nämä kolme ovat erittäin suurten alkulukujen tekijöihin jakamiseen perustuva matemaattinen ongelma (engl. *Integer Factorization Problem*, IFP), diskreetin logaritmin ongelma (engl. *Discrete Logarithm Problem*, DLP) ja elliptisen käyrän ja diskreetin logaritmin ongelmaan perustuva menetelmä (engl. *Elliptic Curve Discrete Logarithm Problem*, ECDLP). [47]

Tässä tutkielmassa esitellään seuraavissa luvuissa IFP:aan perustuva RSA-menetelmä ja DLP:aan perustuva Diffie-Hellman. Nämä kaksi liittyvät läheisesti luvuissa viisi ja kuusi esitettyihin tietoturvaratkaisuihin.

3.2.1 RSA-salausmenetelmä

RSA-salausalgoritmi on yksi yleisimmin käytetyistä epäsymmetrisistä algoritmeista nykyään, koska se on riittävän yksinkertainen, samalla kuitenkin riittävän suojaava ja sen patentti on jo rauennut eli sitä voidaan käyttää vapaasti. RSA:n käyttötarkoitukset ovat digitaalinen allekirjoitus, avainten vaihto ja viestien salaaminen. RSA on de facto -standardi eli mikään virallinen standardointiorganisaatio ei ole standardoinut sitä. RSA:n on julkaistu RSA-DIS -yhtiön *Public Key Cryptography Standards* (PKCS) -sarjassa, jossa on määritelty myös muita algoritmeja [51]. RSA:a käytetään muun muassa IPSecin, *Pretty Good Privacyn* (PGP) ja *Secure Sockets Layerin* (SSL) toteutuksissa. Algoritmiin kehittivät Ron Rivest, Adi Shamir ja Leonard Adleman vuonna 1977. RSA:ssa käytetään nykyään avainpituuksia 1024 bitistä ylöspäin. [47], [78], [27]

RSA-menetelmä perustuu seuraavaan matemaattiseen lauseeseen: [70]

Lause 3.1 *Olkoot p ja q eri alkulukuja, $n = p \cdot q$ ja $m = (p-1)\cdot(q-1)$. Olkoon edelleen kokonaisluku $e \geq 2$ sellainen, että $e \equiv 1 (\bmod n)$, ja kokonaisluku x sellainen, että syt $(x, n) = 1$, missä syt =suurin yhteinen tekijä. Silloin pätee, että $x^e \equiv x (\bmod n)$.*

Ennen viestin salaamista, se on purettava osiin. Osien täytyy olla yhteistä osaa n:ää pienempiä. Seuraavaksi esitän RSA:n periaatteen. [47], [78]

Salaamiseen käytettävä kaava on:

$$C = M^k (\bmod n) \tag{3.1}$$

Purkamiseen käytettävä kaava on:

$$M = C^d (\bmod n) \tag{3.2}$$

Kaavoissa C on salattu viesti, M salattava viesti, e julkinen avain ja d salainen avain. Avainparin yhteinen osa on n eli sitä käytetään sekä salaamisessa että purkamisessa. M:n täytyy olla n:ää pienempi kuten aikaisemmin jo todettiin.

Avaimet e ja d luodaan seuraavalla tavalla. Valitaan kaksi eri alkulukua (yleensä suurta) p ja q, jotka ovat erisuuria. Alkulukujen p ja q tulosta saadaan n. Tämän jälkeen valitaan koodausavain e, jonka tulee myös olla n:ää pienempi ja jolla ei ole yhteisiä tekijöitä luvun $(p-1)\cdot(q-1)$ kanssa. Seuraavaksi lasketaan avain d, joka on muotoa

$$d = e^{-1}(\bmod (p-1)\cdot(q-1)). \tag{3.3}$$

Tällöin käänteislukujen kertolaskun mukaan kaavan

$$e \cdot d = 1(\bmod (p-1)\cdot(q-1)) \tag{3.4}$$

pitää toteutua.

RSA:n toimivuus todistetaan seuraavasti

$$C^d = (M^e)^d = M^{de}. \tag{3.5}$$

Kaavan 3.4 mukaan täytyy olla olemassa sellainen k, että

$$e \cdot d = 1 + k \cdot (p-1)\cdot(q-1), \tag{3.6}$$

joten kaava 3.5 voidaan kirjoittaa muodossa

$$M^{de} = M^{(p-1)\cdot(q-1)\cdot k+1}. \tag{3.7}$$

Edellisestä saadaan muokkaamalla

$$M^{(p-1)\cdot(q-1)\cdot k+1} = M \cdot M^{(p-1)\cdot(q-1)\cdot k}, \tag{3.8}$$

ja koska $M^{(p-1)\cdot(q-1)\cdot k} = 1$ Eulerin teoreeman [47] mukaan, niin

$$M \cdot M^{(p-1)\cdot(q-1)\cdot k} = M(\bmod n) = C^d. \tag{3.9}$$

Kaiken yllä olevan perusteella RSA avaa oikein kaikki luvut M, kun M on välillä $]0, n-1[$.

RSA-menetelmä murtaminen on helposti mahdollista, jos edellisissä kaavoissa esiintyvä n onnistutaan jakamaan tekijöihinsä p ja q. Tällöin salainen avain d saadaan laskettua uudestaan kaavan 3.3 mukaan. RSA:ssa pitääkin valita p ja q niin suuriksi ettei niiden tekijöihin jakaminen onnistu helposti. Tällä hetkellä parhaimmat lukuja tekijöihinsä hajottavat algoritmit ovat aikakompleksisuudeltaan huonompia kuin polynomiaalisia, joten hyvin suurten lukujen tekijöihin jakaminen ei onnistu järkevässä ajassa [71]. Paremman algoritmin olemassaoloa ei ole kuitenkaan pystytty kumoamaan. Jos sellainen löytyisi, pysäyttäisi se kaikkien tekijöihin jakoon perustuvien algoritmien kehittämisen.

Esimerkki 3.1 RSA-algoritmin käyttö pienillä luvuilla [70]

Avainten laskeminen

1. Valitaan kaksi alkulukua $p = 11$ ja $q = 13$.
2. Lasketaan $n = p \cdot q = 143$ ja $m = (p-1) \cdot (q-1) = 120$.
3. Salausavain k s.e. $syt(k, m) = 1$. Valitaan nyt $k = 7$.
4. Lasketaan k:n käänteisalkio k^{-1} renkaassa $\boldsymbol{Z_m}$: Jakoyhtälön mukaisesti $120 = 17 \cdot 7 + 1$, joten $17 \cdot 7 = 120 - 1 \equiv -1 (\operatorname{mod} 120)$. Siten $-17 \cdot 7 \equiv 1$ ja edelleen $(120 - 17) \cdot 7 \equiv 1$ eli $103 \cdot 7 \equiv 1$. Niinpä nyt $k^{-1} = 103$.
5. Laatija (vastaanottaja) antaa lähettäjälle (julkiset avaimet) k ja n. Vastaanottajalle jää (salaiset avaimet) k^{-1} ja $n \cdot k^{-1}$, joiden avulla viesti puretaan.

Viestin lähetys

Lähetyspäässä salainen viesti x koodataan kaavalla

$$r \equiv x^k (\operatorname{mod} n), \tag{3.10}$$

missä r on viesti salattuna. Valitaan nyt $x = 9$, niin $r \equiv 9^7 (\operatorname{mod} 143) \equiv 48$. Nyt salattu viesti r on laskettu ja valmis lähetettäväksi.

Salauksen purku

Vastaanottopäässä viesti puretaan kaavalla

$$r \equiv x^{k^{-1}} (\operatorname{mod} n) \tag{3.11}$$

eli nyt $r \equiv 48^{103} \pmod{143}$ Lasketaan modulo 143

$48^2 \equiv 2404 \equiv 16 \qquad 48^4 \equiv 16^2 \equiv 113 \qquad 48^8 \equiv 113^2 \equiv 42$

$48^{16} \equiv 42^2 \equiv 48 \qquad 48^{32} \equiv 48^2 \equiv 16 \qquad 48^{64} \equiv 16^2 \equiv 113$

ja siten

$48^{103} \equiv 48^{64+32+4+2+1} \equiv 48^{64} \cdot 48^{32} \cdot 48^4 \cdot 48^2 \cdot 48 \equiv 113 \cdot 16 \cdot 113 \cdot 16 \cdot 48 \equiv 9$

eli $x = 9$.

3.2.2 Diffie-Hellman -algoritmi

Diffie-Hellman on myös RSA:n tavoin de facto -standardi ja kuuluu PKCS-standardeihin. Diffie-Hellman perustuu aikaisemmin mainittuun DLP:aan eli diskreetin logaritmin ongelmaan. Diffie-Hellman -algoritmi määrittelee turvallisen mekanismin avainten jakeluun. Tämä ratkaisee symmetrisissä salausalgoritmeissa tarvittavan avainten jakelun.

Diffie-Hellman toimii siten, että molemmat kommunikoinnin osapuolet voivat saada salaisen avaimen, vaikka salaista tietoa ei vaihdeta ollenkaan. Diffie-Hellman ei toteuta osapuolten tai viestien todennusta, koska siinä ei käytetä mitään ennakkotietoja. Se on siis altis välimieshyökkäykselle, jossa kolmas epäilyttävä osapuoli kuuntelee kommunikointia ja muokkaa viestejä omaksi edukseen. Hyökkääjän (M) täytyy päästä käsiksi kumpaankin suuntaan kulkevaan liikenteeseen. Henkilön A lähettäessä viestiä B:lle M nappaa viestin ja muuntaa viestissä olevan A:n julkisen luvun omaksi julkiseksi luvukseen. M saa viestin ja luulee, että kyseinen luku on A:n. Nyt B puolestaan lähettää oman lukunsa A:lle, mutta M kaappaa senkin ja muuntaa tilalle oman lukunsa. Näin ollen M pystyy jatkossa seuraamaan A:n ja B:n välistä liikennettä ja tarpeen mukaan muokkaamaan sitä. Todennus onkin toteutettava muulla tavoin, jotta algoritmista saadaan luotettava.

Algoritmin toiminta [51], [59]

Osapuolet A ja B keskustelevat salaamattomalla kanavalla.

1. Osapuolet muodostovat julkiset luvut α ja p, missä p on suuri alkuluku ja α on äärellisen kunnan (*Galoisin kunta*, GF) $GF(p)$:n primitiivielementti eli luku,

joka generoi kaikki muut $GF(p)$:n elementit $(1, 2, 3, ..., p-1)$. Yleensä toinen osapuolista luo nämä luvut ja lähettää ne sitten toiselle.

2. A generoi itselleen yhden ison satunnaisluvun x ja lähettää sen B:lle muodossa

$$X = \alpha^x \bmod p, \tag{3.12}$$

jolloin kuuntelija ei pysty saamaan selville sitä. X on määritelty $GF(p)$:ssä eli kunnassa $\boldsymbol{Z}_p^*$.

3. B generoi itselleen yhden ison satunnaisluvun y salaiseksi luvukseen ja lähettää sen A:lle muodossa

$$Y = \alpha^y \bmod p. \tag{3.13}$$

Nytkään kolmas osapuoli ei pysty päättelemään salaista lukua Y:stä. Myös Y on määritelty $GF(p)$:ssä.

4. Lopuksi osapuolet laskevat itselleen yhteisen salaisen avaimen K. A laskee seuraavasti

$$K = Y^x \bmod p \tag{3.14}$$

ja B seuraavasti

$$K = X^y \bmod p = (\alpha^x \bmod p)^y \bmod p) = (\alpha^y)^x \bmod p = (\alpha^y \bmod p)^x \bmod p = Y^x. \tag{3.15}$$

Molempien saamat K:n arvot ovat siis samat ja niitä voi käyttää salaisena avaimena.

Diffie-Hellmanin voidaan käyttää myös muissa ryhmissä, joissa sekä DLP että potenssiin korotus on tehokas. [59]

3.3 Tiivistefunktiot

Tiiviste- eli hash-funktiot (käytetään myös hajautusfunktio, hajautus-, tiiviste- ja hash-algoritmi sanoja) ovat yksisuuntaisia funktioita. Yksisuuntaisuus tarkoittaa ettei lopputuloksesta voi päätellä alkuarvoa. Hash-funktioilla lasketaan tiivistesumma, jonka perusteella voidaan tarkistaa esimerkiksi IP-paketin eheys. Vastaanottaja tarkistaa paketin laskemalla tiivisteen uudestaan ja vertaamalla sitä lähettäjältä saamaansa tiivisteeseen. Tiivistefunktiot eivät tarvitse salaista avainta tiivisteen (eheyssumma) laskemiseen. Esittelen seuraavaksi pari tunnettua tiivistefunktiota, joita käytetään myöhemmin esiteltävissä tietoturvamekanismeissa. [51]

3.3.1 Message Digest 5 (MD5) ja Secure Hash Algorithm 1 (SHA-1)

MD5 ja SHA-1 ovat *Message Digest 4:ään* (MD4) perustuvia tiivistefunktioita. Ne ovat tällä hetkellä suosituimpia tiivistefunktioita. MD4 ja MD5 ovat Ron Rivestin, joka on myös RSA:n yksi kehittäjistä, kehittämiä. SHA-1 [75] on puolestaan NIST:n kehittämä. SHA-1 on muunnos alkuperäisestä SHA:sta. SHA-1:ssä on poistettu SHA:n heikkouksia lisäämällä siihen yhden bitin rotaatio. MD5 ja SHA-1 ovat käytössä monissa sovelluksissa ja ne vaaditaan myös tehtäväksi IPSecin [6], [7] toteutuksiin. [59], [69], [78]

3.3.2 Muita tiivistefunktioita

Muita yleisesti käytettyjä tiivistefunktioita ovat RIPEMD ja SHA-2, koska ne antavat paremman suojan törmäyksiä vastaan kuin MD5 ja SHA-1 pidemmällä tiivisteellä käytettynä. RIPEMD-160:tä käytettäessä tulee 160 bittinen tiiviste ja SHA-2-256:sta käytettäessä 256 bittinen. Funktioilla voidaan tuottaa myös muun pituisia tiivisteitä. Myös nämä kaksi funktiota perustuvat MD4:ään. RIPEMD on kehitetty Euroopan unionin RIPE-projektissa. [59], [51]

3.3.3 Yhteenveto

Lopuksi esitän vertailun eri tiivistefunktioista. MD4 on erittäin nopea, mutta se on jo todettu turvattomaksi ja sitä ei enää käytetä. Sen nopeasti korvannut MD5 on myös nopea, mutta sen tuoma turva ei ole yhtä hyvä kuin SHA-1:n, SHA-2:n tai RIPEMD-160:n. SHA-1 ja RIPEMD-160 ovat hitaimpia, mutta ne antavat paremman suojan kuin nopeammat ja lyhyemmän tiivisteen tekevät funktiot. [59]

Nimi	Tiivisteen pituus	Suhteellinen nopeus
MD4	128	1.00
MD5	128	0.68
RIPEMD-128	128	0.39
SHA-1	160	0.28
RIPEMD-160	160	0.24
SHA-2-256	256	-

Taulukko 3.2: Tiivistefunktioiden vertailu, [59]

Taulukossa 3.2 on yleisimpien tiivistefunktioiden vertailu. Siinä nopeudet on laskettu suhteellisina siten, että MD4 on nopein arvolla 1. Tiivisteen pituudesta, joka on laskettu bitteinä, pystyy arvioimaan funktion vahvuutta. Mitä pidempi tiiviste, sitä vahvempi suoja. [59]

3.4 Viestien todennus

Viestien todennus tarkoittaa sitä, että viestin lähettäjä pystytään tunnistamaan varmasti ja että pystytään todistamaan ettei viestiä ole muutettu matkalla. Digitaalinen allekirjoitus puolestaan on todennustekniikka, johon sisältyy lähettäjän osallisuuden kiistämättömyys.

Todennusfunktiot ovat funktioita, jotka tuottavat todennussumman. Todennussumman perusteella vastaanottaja kykenee todentamaan viestin. Todennusfunktiot voidaan jakaa seuraaviin kolmeen luokkaan [78]:

- *Viestin salaus*: Koko viestin salattu versio toimii todennussummana.
- *Message Authentication Code* (MAC): Julkinen funktio tuottaa salaisen avaimen avulla viestistä kiinteän pituisen summan, joka toimii todennussummana.
- *Tiivistefunktio*: Julkinen funktio, joka kuvaa viestin kiinteän pituiseksi tiivisteeksi. Tiiviste toimii eheys- ja todennussummana.

3.4.1 Todennus viestin salauksella

Symmetrinen salaus

Tarkastellaan perinteistä salausta salaisella avaimella. Siinä viestin salaamisella saavutetaan luottamuksellisuus. Muut kuin lähettäjä ja vastaanottaja ei pysty lukemaan viestiä. Myös lähettäjä pystytään päättelemään. Koska muut ei tiedä salaista avainta, lähettäjän on pakko olla sama, jonka kanssa yhteinen avain on sovittu. Salattua viestiä ei pysty muokkaamaan järjellisesti ilman, että tietää salaisen avaimen ja muokkaa viestiä selväkielisenä. Tästä johtuen vastaanottaja tietää saadessaan purettua salatun viestin järjellisesti auki ettei se ole muuttunut matkalla. Kaikki edelliset yhdistettynä voimme sanoa, että perinteinen salaus toteuttaa viestin todennuksen ja luottamuksellisuuden. [78]

Todennus ei kuitenkaan ole niin selkeä symmetrisen salauksen tapauksessa. Jos viestin sisältö on esimerkiksi kuva, ei siitä pysty sanomaan onko sitä muutettu pelkästään edellisen perusteella. Nyt tähän menetelmään jää siis aukko, jota mahdolliset hyökkääjät pystyvät hyödyntämään esimerkiksi DoS-hyökkäyksessä. On vaikeaa todeta automaattisesti, mikä on kelpo viesti ja mikä ei. Tämä ongelma voidaan korjata antamalla selväkieliselle tekstille jokin rakenne, joka on helposti tunnistettavissa, mutta jota ei voida tehdä kuin selväkielisenä. Tästä voidaan pitää esimerkkinä jotakin virheenkorjaukseen liittyvää tarkistussummaa. Tarkistussumman avulla voidaan katsoa salauksen purkamisen jälkeen automaattisesti onko viesti järjellinen. Toinen esimerkki, jolla voidaan parantaa todennuksen luotettavuutta, on TCP/IP-perheen kehysrakenteen käyttäminen viestissä. Tästä voidaan pitää esimerkkinä tilannetta, jossa salataan kaikki muu paitsi IP-otsikko. Tällöin voidaan todeta muun muassa TCP:n otsikosta sen kenttien avulla, että kaikki on kunnossa. [78]

Epäsymmetrinen salaus

Epäsymmetrisellä salauksella toteutetaan todennus siten, että lähettäjä salaa omalla salaisella avaimellaan viestin ja vastaanottaja purkaa sen lähettäjän julkisella avaimella. Tällöin vastaanottaja voi olla varma lähettäjästä, koska kellään muulla kuin lähettäjällä ei ole mahdollisuutta tehdä viestiä hänen salaisella avaimellaan. Tämä ei kuitenkaan toteuta luottamuksellisuutta.

3.4.2 Message Authentication Code (MAC)

MAC eli eheys- ja todennussumma lasketaan jollakin funktiolla, jossa on syötteenä salainen avain ja todennettava viesti. Funktio tekee kaikista syötteistä samanpituisen summan (tiiviste). Vastaanottaja todentaa viestin laskemalla MAC:n uudestaan ja vertaamalla sitä lähettäjältä saamaansa. Perinteisesti MAC on laskettu jonkin symmetrisen salausalgoritmin kuten DES:n avulla. Symmetrisen salausalgoritmin käyttö ei ole kuitenkaan niin selvää tässä tarkoituksessa kuten aikaisemmin jo todettiin. Nykyään yleisin käytössä oleva tapa käyttää MAC:a onkin Keyed-hash Message Authentication Code (HMAC). [78]

Keyed-hash Message Authentication Code (HMAC)

HMAC-funktio on mekanismi viestien todentamiseksi käyttämällä tiivistefunktiota yhdessä salaisen avaimen kanssa. HMAC:n avulla voidaan todennussumma laskea käyttäen salaista avainta ja vapaavalintaista tiivistefunktiota. Muun muassa MD5:n, SHA-1:n ja RIPEMD:n käyttö HMAC:n ja IPSecin kanssa on määritelty [37], [38], [52]. HMAC on tehty siten, että minkä tahansa tiivistefunktion käyttö on sen kanssa helppoa. Tämä on tehty sen vuoksi, että tiivistefunktiot kehittyvät koko ajan ja paremman suojan antavia funktioita voidaan siten ottaa nopeammin käyttöön. HMAC:n tarjoaman suojan vahvuus siis riippuu tiivistefunktion ominaisuuksista. HMAC:lla pystytään todentamaan sekä viestin eheys että alkuperä. [16], [78]

HMAC:a vastaan on hankala hyökätä. Hyökkääjän on pystyttävä laskemaan HMAC, vaikka HMAC:n alustusvektori on satunnainen ja salainen avain ovat tuntemattomia. Toinen hyökkäystapa on etsiä törmäyksiä, vaikka HMAC:n alustusvektori on satunnainen ja salainen. [78]

3.4.3 Tiivistefunktiot

Yksi todennukseen käytetyistä tavoista on yksisuuntainen tiivistefunktio. Tiivistefunktion ominaisuuksista kerrottiin alaluvussa 3.3. Tiivistefunktiolla saadaan viestistä kiinteän pituinen tiiviste eli eheyssumma. Tiivistefunktiota ei voida käyttää yksinään viestin todennukseen vaan se toimii todennusmekanismin osana. Tiivistefunktioita voidaan käyttää seuraavilla tavoilla todennuksessa [78]:

- Viestiin lisätään eheyssumma ja sen jälkeen niiden yhdistelmä salataan symmetrisellä salauksella. Vastaanottaja pystyy nyt toteamaan alkuperän, koska salainen avain on vain osapuolten tiedossa ja eheyssumma tuo määrätyn rakenteen viestiin. Tästä mainittiin jo *symmetrisen salauksen käyttö todennuksessa* -kohdassa.
- Vain eheyssumma salataan symmetrisellä salauksella jolloin tuloksena on MAC, josta kerroin jo alaluvussa 3.4.2.
- Vain eheyssumma salataan epäsymmetrisellä salauksella käyttämällä lähettäjän salaista avainta. Tämä toteuttaa viestin alkuperän tunnistuksen kuten edellisessä kohdassa, mutta sen lisäksi tämä toteuttaa digitaalisen allekirjoituksen. Näin on, koska vain lähettäjällä on hallussaan salainen avain, jolla eheyssumma on salattu.
- Osapuolet jakavat yhteisen salaisuuden. Sen ja viestin yhdistelmästä lasketaan eheyssumma ja se lisätään viestiin. Koska vastaanottaja tietää yhteisen salaisuuden, pystyy se laskemaan vastaavan eheyssumman ja toteamaan viestin tulleen toiselta osapuolelta. Muut eivät pysty laskemaan kyseistä eheyssummaa, koska ne eivät tiedä jaettua salaisuutta. HMAC perustuu tämän kaltaiseen mekanismiin, mutta on monimutkaisempi.

Tiivistefunktioiden käyttöä puoltaa niin nopeus verrattuna salausalgoritmeihin kuin myös monien maiden vientirajoitukset salausalgoritmeille. Tiivistealgoritmien vientiä ei ole yleensä rajoitettu mitenkään. [78]

3.5 Hyökkäyksiä

Eri hyökkäyksiä käytiin läpi toisessa luvussa. Nyt esittelen, miten ne liittyvät tässä luvussa esiteltyihin kryptografisiin algoritmeihin.

3.5.1 Salausalgoritmit

Salattuihin viesteihin kohdistuvat hyökkäykset jaetaan päätyyppeihin [51]:

- *Tunnetun sanoman murto* – murtautuja tuntee algoritmin ja hänellä on hallussaan jonkun verran algoritmilla salattua viestiä. Hän ei tunne selväkielisanomaa eikä hänellä ole hallussaan salaista avainta.
- *Tunnetun selväkielisanoman murto* – murtautujalla on hallussaan jonkun verran salattua viestiä ja vastaava selväkielisenä. Murtautuja tuntee algoritmin, mutta ei avainta. Tehtävänä on löytää avain, jotta pystytään purkamaan lisää salattua viestiä.
- *Valitun selväkielisanoman murto* – murtautuja pääsee käsiksi valittua selväkielisanomaa vastaavaan salasanomaan. Murtautuja tuntee algoritmin, mutta ei avainta. Tehtävänä on löytää avain, jotta pystytään purkamaan lisää salattua viestiä.
- *Adaptiivinen valitun selväkielisanoman murto* on edellisen tapauksen erikoistapaus, jossa murtautuja valitsee seuraavan salattavan viestin edellisen salauksen tuloksen perusteella.
- *Valitun salasanoman murto* – murtautuja pääsee käsiksi valitsemaansa salattua viestiä vastaavaan selväkieliseen sanomaan.

Lisäksi voidaan *raa'an voiman murtoa* (engl. *brute-force attack*) eli murtoa laskentatehoa käyttämällä pitää yhtenä tyyppinä. Menetelmää käytettäessä käydään läpi kaikki salausavaimet ja verrataan purettua viestin osaa johonkin tunnettuun tai tutkitaan muuten, onko viesti järkevä.

Edellisissä kohdissa yritetään saada selville viestin sisältö eli ne ovat hyökkäyksiä luottamuksellisuutta vastaan. Hyökkäys tapahtuu passiivisesti kuuntelemalla ja/tai aktiivisesti lähettämällä jokin haluttu viesti, joka tulee salatuksi.

Liikenteen analysointia voi tehdä vaikka liikenne olisikin salattua. Liikenteestä ei vain pysty päättelemään aivan yhtä paljon asioita. Hyökkääjälle hyödyllisiä tietoja kuten viestin vastaanottaja ja viestien määrä on vaikea piilottaa salaamalla, koska jotenkin se liikenne on ohjattava perille.

3.5.2 MAC ja tiivistefunktiot

MAC ja eheyssummiin kohdistuvat kaksi perushyökkäystä, jotka ovat erityisiä tiivistefunktioille, kuvataan tässä.

Satunnaishyökkäyksen (engl. *random attack*) tapauksessa hyökkääjä valitsee satunnaisen viestin, muokkaa sitä ja toivoo ettei muutosta huomata. Turvallisen tiivistefunktion tapauksessa tämän onnistumisen todennäköisyys on $1/2^n$, missä n on tiivisteen pituus bitteinä. [40]

Toinen perushyökkäys on *syntymäpäivähyökkäys* (engl. *birthday attack*). Syntymäpäivähyökkäyksen idea on se, että todennäköisyys sille, että 23 hengen ryhmässä ainakin kahdella on sama syntymäpäivä, ylittää 1/2. Tämä saadaan laskemalla ensin todennäköisyys $Q(h, 365)$ kaavalla 3.16 sille, että kaikilla on eri syntymäpäivä

$$Q(h, 365) = \frac{365-1}{365} \cdot \frac{365-2}{365} \cdots \frac{365-(h-1)}{365} = \frac{(365-1)(365-2)\cdots[365-(h-1)]}{365^{h-1}}, \tag{3.16}$$

missä h on henkilöiden lukumäärä.

Tämä voidaan kirjoittaa muotoon

$$Q(h, 365) = \frac{365!}{(365-h)!365^h} \tag{3.17}$$

Edellisen perusteella lasketaan seuraavasti todennäköisyys P(h,365) sille, että vähintään kahdella on sama syntymäpäivä

$$P(h, 365) = 1 - Q(h, 365) = 1 - \frac{365!}{(365-h)!365^h}. \tag{3.18}$$

Sijoittamalla edelliseen lauseeseen h:n paikalle 22 ja 23 huomataan, että 23 on ensimmäinen henkilömäärä, jolloin todennäköisyys ylittää 1/2.

Syntymäpäivähyökkäystä voidaan soveltaa tiivistefunktioita vastaan seuraavasti: hyökkääjä generoi r_1 muunnelmaa tekaistusta viestistä ja r_2 muunnelmaa aidosta viestistä. Todennäköisyys löytää sellainen tekaistu ja aito viesti, että tiivistesumma on sama, saadaan kaavasta

$$1 - \exp\left(\frac{-(r_1 \cdot r_2)}{2^n}\right). \tag{3.19}$$

Kun $r = r_1 = r_2 = 2^{n/2}$, todennäköisyys on noin 63%. Vertailuongelma ei vaadi vaativuudeltaan r^2 operaatioita. Datan lajittelun, vaativuudeltaan $O(r \log r)$, jälkeen vertailu on helppoa. Jos tiivistefunktiota pystytään kutsumaan mustan laatikon

-periaatteella eli ei tiedetä, miten algoritmi toimii, vaatii se $2 \cdot \sqrt{\frac{\pi}{2} \cdot 2^{n/2}}$ operaatiota ja vähäpätöisen määrän muistia. Johtopäätöksenä voidaan vetää, että turvallisuuden takaamiseksi pitää käyttää ainakin 128 bittiä pitkiä tiivisteitä. [40]

Nämä hyökkäykset ovat aktiivisia (muuntaminen ja väärennös) ja koskevat eheyttä ja todennusta. Hyökkäykset vaativat lisäksi hyökkääjältä pääsyä kaappaamaan liikennettä ja lähettämään se uudelleen tai pelkästään lähettämään tekaistu viesti tekaistulla kryptografisella summalla varustettuna.

4 Internet Protokolla (IP) ja verkonhallinta

4.1 TCP/IP-protokollaperhe

Internet Protokolla (IP) on koko Internetin ydin, mutta se ei yksinään pysty tarjoamaan kaikkia tarpeellisia palveluita. Se vuoksi on kehitetty *TCP/IP-protokollaperhe*. TCP/IP tarkoittaa IP:n ympärille rakentunutta protokollaperhettä, jossa IP toimii *verkkokerroksella* ja *Transmission Control Protocol* (TCP) tai *User Datagram Protocol* (UDP) kuljetuskerroksella. TCP on yhteydellinen tiedonsiirtoprotokolla ja UDP vastaava yhteydetön. Sovelluskerroksella toimii esimerkiksi *Simple Network Management Protocol* (SNMP) ja *File Transfer Protocol* (FTP). [50]

Kuvassa 4.8 näkyy TCP/IP-protokollakerrosten sijainti verrattuna ISO:n *Open Systems Interconnection* (OSI) -malliin. OSI-malli oletetaan lukijoille jo tutuksi. TCP/IP on pyritty tekemään yksinkertaiseksi ja siinä onkin vähemmän kerroksia kuin OSI:ssa - vain neljä OSI:n seitsemää vastaan. TCP/IP:n kerrosten tehtävät ovat lähes samat kuin samalla kohdalla kuvassa 4.8 olevien OSI-kerrostenkin. [50]

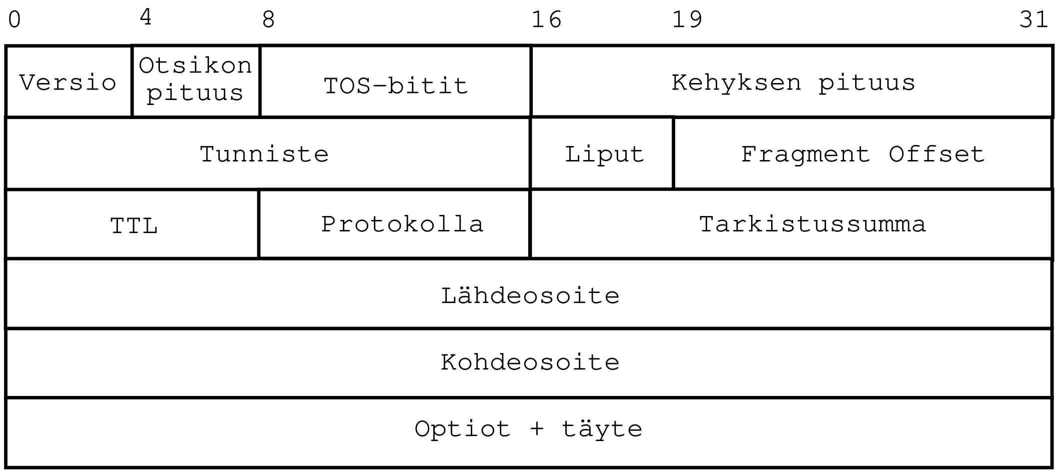
Kuva 4.8: TCP/IP:n protokollakerrokset verrattuna OSI-mallin kerroksiin [50]

Jokaisen TCP/IP-kerroksen protokolla tai protokollat, joiden kautta tieto kulkee, lisäävät oman otsikkonsa pakettiin. Kun lähetettävä tieto lähtee sovellukselta, ensimmäisenä sen eteen [5] laittaa oman otsikkonsa sovellusprotokolla. Seuraavaksi sovellusprotokollan kehystämään pakettiin lisää oman otsikkonsa kuljetuskerroksen protokolla, esim. TCP. Verkkokerroksella viimeisenä varsinaisena TCP/IP-protokollaperheen jäsenenä IP lisää oman otsikkonsa TCP-kehykseen jolloin IP-paketti on valmis lähetettäväksi eteenpäin. Tämän jälkeen IP-pakettiin lisätään linkkikerroksen otsikko (esim. Ethernet), joka ei enää kuulu TCP/IP-perheeseen. Vastaanottopäässä otsikot poistetaan päinvastaisessa järjestyksessä ja annetaan kehys aina ylempänä mallissa sijaitsevalle protokollalle.

Tämän tutkielman kannalta Internet Protokolla on tärkein TCP/IP-perheen protokollista. IP versio 4 (IPv4) on toistaiseksi yleisin IP:n versio ja se esitellään seuraavassa alaluvussa. Ensiksi esitellään otsikon rakenne, sen jälkeen IP:n ominaisuudet ja palvelut. Lopuksi kerrotaan tietoturvaongelmista ja IPv4:n tulevaisuudesta.

4.2 IPv4

4.2.1 Rakenne



Kuva 4.9: IP:n otsikko [50]

Versio

Versio kertoo IP:n versionumeron ja se on 4 IPv4:n tapauksessa.

[5] Jotkin protokollat lisäävät tietoa myös loppuun.

Otsikon pituus

Otsikon pituus kertoo IP-otsikon pituuden 32 bittisinä sanoina. Otsikon maksimipituudeksi muodostuu 60 oktettia, koska kentän pituus on 4 bittiä. Otsikon pituuteen lasketaan myös *Optiot*.

Type Of Service (TOS)

TOS on 8 bittiä pitkä. Kentän TOS-biteillä voidaan ryhmitellä IP-paketteja esimerkiksi niiden vaatiman palvelun laadun mukaan.

Kehyksen pituus

Kehyksen pituus kerrotaan 16 bitin kentässä. Pituus ilmoitetaan oktetteina. Edelliset tiedot yhdessä asettavat IP-paketin maksimikooksi 65535 oktettia, mutta käytännössä ei voi kuitenkaan käyttää niin pitkiä paketteja, koska TCP/IP-pinon ei ole pakko kyetä vastaanottamaan kuin 576 oktetin paketteja.

Tunniste

16 bittiä pitkä *Tunnistekenttä* yksilöi samasta ylemmän kerroksen datasta pilkotut kehykset vastaanottopäätä varten, jotta vastaanottaja tietää mitkä paketit kuuluvat samaan ylemmän kerroksen dataan.

Liput

Liput ovat myös datan pilkkomiseen liittyviä bittejä. Kenttä sisältää kolme bittiä, joista ensimmäisen käyttöä ei ole määritelty. Toinen bitti, M-bitti, kertoo, että kyseisen paketin jälkeen on vielä tulossa paketti, joka kuuluu samaan isompaan alkuperäiseen IP-pakettiin. Kolmas bitti, D-bitti, ilmoittaa ettei pakettia saa pilkkoa pienempiin osiin.

Fragment offset

Fragment offset -kenttä kertoo pilkottujen pakettien järjestyksen. Kenttä on 13 bittiä pitkä.

Time To Live (TTL)

TTL kertoo kuinka monen laitteen kautta IP-paketti saa vielä kulkea. Arvon mennessä nollaan paketti tuhotaan. Tyypillinen arvo on 255, joka on 8 bittisen kentän suurin mahdollistama arvo.

Protokolla

Protokolla tarkoittaa ylemmän kerroksen protokollan, joka antoi datan IP:lle, tunnistetta.

Tarkistussumma

Tarkistussumma on IP-otsikosta laskettu tarkistussumma. Datan tarkistus kuuluu ylemmille kerroksille.

Lähde- ja *kohdeosoitteet*

Lähde- ja *kohdeosoitteet* on 32 bittisiä. Kerron niistä enemmän seuraavassa alaluvussa.

Optiot ja *täyte*

Viimeisinä kenttinä tulee mahdolliset *Optiot* ja *täyte*. Optiot on varattu IP:lle suunnitelluille valinnaisille toiminnoille. Näitä ei kuitenkaan juurikaan käytetä. Täytettä lisätään, jos otsikko ei lopu 32 bitin monikertaan.

4.2.2 Osoitteet

IPv4:ssä on käytössä 32-bittiset osoitteet. Niiden määrä on kuitenkin havaittu riittämättömäksi ja nykyään onkin monessa organisaatiossa käytössä *osoitteenmuunnokset* (engl. *Network Address Translation*, NAT). Toinen keino lisätä osoitteiden käyttöastetta on vaihtuvanmittaisien aliverkkomaskien käyttö reitityksessä (engl. *Classless Inter-Domain Routing*, *CIDR*).

IP-osoitteet ovat muotoa $x.x.x.x$, missä x on 8 bitin kuvaama kokonaisluku. Esimerkkeinä osoitteista ovat 130.234.1.1 ja 192.168.100.102. IP-osoitteet ovat globaalisti yksikäsitteisiä joitain poikkeuksia lukuun ottamatta. IPv4-osoitteet jaetaan luokkiin taulukon 4.3 mukaan. Varatut villit osoitteet on esitetty taulukossa 4.4.

Verkkoluokka	Varatut osoitteet	Verkkoja	Laitteita/verkko
Ko. verkko itse	0.0.0.0		
A-luokka	1.x.x.x – 126.x.x.x	126	1677214
Takaisinkytkentä	127.x.x.x		
B-luokka	128.x.x.x – 191.x.x.x	16384	65534
C-luokka	192.x.x.x – 223.x.x.x	2097152	254
D-luokka (ryhmälähetys)	224.x.x.x – 239.x.x.x		
E-luokka (kokeilukäyttö)	240.x.x.x – 255.x.x.254		
Levitysviesti	255.255.255.255		

Taulukko 4.3: IPv4-osoiteluokat [50]

Muita erityisiä IP-osoitteita on myös olemassa. Jos ensimmäinen luku on 127, kyseeessä on silloin takaisinkytketty osoite. Tällaiset osoitteet ohjataan koneeseen itseensä. Osoite 255.255.255.255 on puolestaan *yleislähetysosoite* (engl. *broadcast*). Jos osoitteen bitit ovat nollia, tarkoitetaan sillä verkkoa itseään. Niitä käytetään esimerkiksi reititystauluissa kuvaamaan aliverkkoja. Osoitteet väliltä 224.0.0.0 – 239.255.255.255 on varattu *ryhmälähetyksiä* (engl. *multicast*) varten. Lisäksi kokeilukäyttöön on varattu osoitteet väliltä 240.0.0.0 – 255.255.255.254.

Verkkoluokka	Varatut osoitteet	
A-luokka	10.0.0.0 – 10.255.255.255	(10/8)
B-luokka	172.16.0.0 – 172.31.255.255	(172.16/12)
C-luokka	192.168.0.0 – 192.168.255.255	(192.168/16)

Taulukko 4.4: RFC1918:n varaamat villit IPv4-osoitteet [50]

4.2.3 Palvelut

IPv4 tarjoaa kuljetuspalvelua ylemmille kerroksille. Yleensä kohteeseen reititys tapahtuu kohdelaitteen osoitteen perusteella. IPv4 tarjoaa muina lähetysmuotoina ryhmä- ja yleislähetyksiä, joissa voi olla useampia vastaanottajia. Reitityksestä kerron tarkemmin seuraavassa kappaleessa.

Reititys tarkoittaa mekanismia, jolla paketti ohjataan lähettäjältä vastaanottajalle kohdeosoitteen perusteella. Reititys voidaan jakaa kahteen osa-alueeseen. Ensimmäinen osa-alue on paketin ohjaaminen sisääntuloliitännästä oikeaan ulostuloliitäntään ja toinen on reititystaulutietojen vaihtaminen muiden reitittimien kanssa. Reitittimet ovat siis laitteita, jotka ohjaavat paketteja kohti oikeaa kohdeosoitetta. Tässä tutkielmassa ei mennä syvemmälle reitityksen toteutukseen.

IP ei takaa mitenkään kuljettamansa datan oikeellisuutta. Se tarkistaa kuitenkin oman otsikkonsa. Datan oikeellisuuden tarkistukseen käytetään ylempiä protokollia.

Pakettien *pilkkominen* (engl. *fragment*) pienempiin osiin, jos verkko ei voi kuljettaa niin suuria paketteja, on yksi IPv4:n palveluista. Vastaanottopäässä paketit vastaavasti kootaan IPv4:n toimesta takaisin isommiksi.

4.2.4 Tietoturva

IPv4:stä löytyy monia puutteita, joita voi hyödyntää erilaisilla hyökkäyksillä. Esittelen seuraavaksi näitä hyökkäyksiä. Joukossa on myös yleisesti TCP/IP-protokollaperhettä koskevia hyökkäyksiä.

Lähdeosoitteen väärentäminen

IP-paketissa olevan IP-lähdeosoitteen voi väärentää (engl. *IP-spoofing*). UDP-paketissa kerrottua IP-osoitetta käytetään vastauksien lähettämiseen ja siinä ei tarvita yhteydenmuodostusta, joten UDP:a vastaan on helppo hyökätä. Riittää, kun hyökkääjä asentaa koneelleen hyökkäysohjelmiston, joka osaa lähettää tietynlaisia UDP-paketteja väärällä lähdeosoitteella. IP-lähdeosoitteen väärentämisellä voidaan kiertää IP-osoitteisiin pohjautuvat pääsynvalvontamenetelmät. Riittää siis esimerkiksi väärentää palvelupyyntö paikallisverkosta tulevaksi, vaikka todellisuudessa pyyntö tulee ulkoa. Tämä pystytään kuitenkin estämään tarkastamalla liikenne jo reitittimellä tai palomuurilla ja suodattamalla ulkopuolelta sisäverkon osoitteella tulevat paketit. [62]

Vastaanotto-osoitteen väärentäminen (ARP-huijaus)

Ethernet-verkkoon liittyvä huijaus perustuu verkossa olevien koneiden tapaan ilmoittaa oma Ethernet-osoite, kun kuulee kyseltävän omaa IP-osoitettansa. Ethernet verkossa IP-paketteja liikutetaan Ethernet-laiteosoitteen perusteella ja kun huijari on ehtinyt ilmoittaa oman Ethernet-osoitteensa ennen oikeata IP-osoitteen haltijaa, saa hän kyseisen IP-osoitteen paketit itselleen. Näihin osoitteiden kyselyihin ja vastauksiin käytetään *Address Resolution Protokollaa* (ARP) ja siitä tulee nimi ARP-huijaus. [62]

Nauhoitushyökkäys

Nauhoitushyökkäys eli toistohyökkäys esiteltiin jo luvussa kaksi. Tallentamalla oikein muotoiltuja viestejä verkosta ja lähettämällä niitä uudelleen saadaan aikaan keskeytyshyökkäys (DoS-hyökkäys). Tämä toimii, koska IPv4:ssä ei ole juoksevaa numerointia paketeille eli vastaanottaja olettaa paketin aina uudeksi. TCP:tä vastaan hyökättäessä pitää sekvenssinumeroa kasvattaa oikein, jotta hyökkäys onnistuisi. Tämän muuntaminen puolestaan onnistuu, koska paketti sisältöä ei todenneta mitenkään. [62]

ICMP-hyökkäykset

Internet Control Message Protokolla (ICMP) on IP-tasolla toimiva ohjaus- ja hallintaprotokolla. ICMP:ssa on Redirect-toiminta, joka tarkoittaa uudelleenohjausta. Sen avulla hyökkääjä voi uskotella, että hänen kauttansa löytyy lyhyempi reitti kuin jonkin toisen reitittimen kautta. Jos kohde uskoo hyökkääjän olevan reititin ja alkaa lähettämään tälle paketteja, voi hyökkääjä yrittää saada myös paluupaketit huijaamalla oman osoitteensa. [62]

ICMP:aa käytetään myös DoS-hyökkäyksiin. Sillä pystyy lähettämään *echo request* -viestejä, joihin hyökkäyksen kohde vastaa ja tukkii näin omaa verkkoliityntäänsä. Näissä ICMP echo request -viesteissä on väärennetty lähdeosoite ja tämä toimii samalla hyökkäyksenä väärennettyyn osoitteeseen. Parhaiten tämä hyökkäys toimii hajautettuna, koska se kuluttaa myös hyökkääjältä kapasiteettia. [13]

ICMP:aa voidaan käyttää myös verkon skannaukseen, jolla pyritään selvittämään verkon rakenne. Palomuureja konfiguroitaessa pitää miettiä tarkkaan, mitä tyyppejä ICMP:sta päästää läpi. Aiheesta on kerrottu lisää lähteessä [13].

Salakuuntelu

Salakuuntelu rikkoo luottamuksellisuuden ja on helppoa, jos hyökkääjän kone sijaitsee samassa Ethernet-segmentissä tai pääsee muuten fyysisesti käsiksi kaapelointeihin. Viestejä ei ole salattu IPv4:ssä, joten salakuuntelija voi lukea suoraan pakettien sisällön. Salakuuntelemalla voi etsiä esimerkiksi käyttäjien salasanoja, jotka liikkuvat verkossa suojaamattomana. [62]

Nimipalvelun väärentäminen

Internetin nimipalvelun väärentäminen on yksi tapa ohjata paketteja väärään osoitteeseen. Nimipalvelun väärentämiskohteita ovat joko IP-osoitetta koskeva domainnimi tai toisinpäin. Tätä vastaan voi suojautua tekemällä kyselyn molemmin päin. Jos koko nimipalvelu on väärennetty, sille ei mahda mitään. [62]

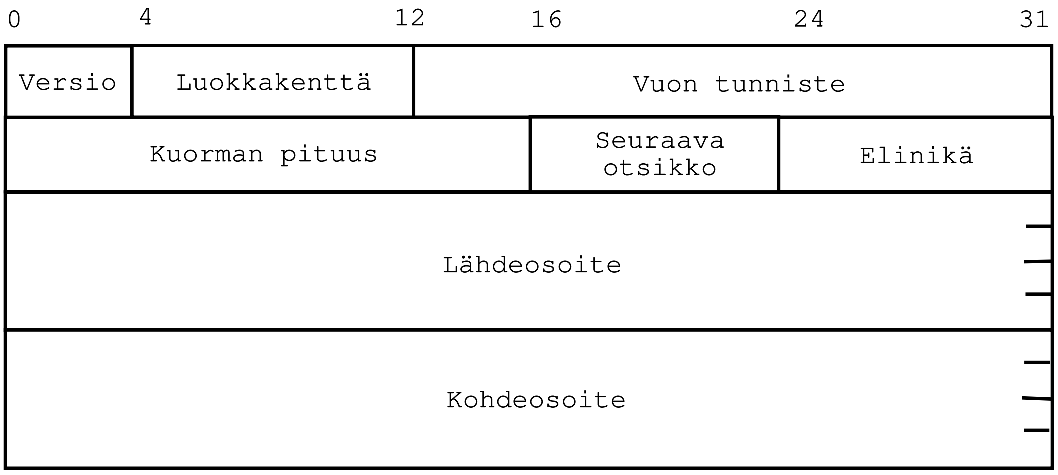
4.2.5 Tulevaisuus

IPv4 on tulossa pikkuhiljaa tiensä päähän. IPv4-osoitteita ei enää riitä muutaman vuoden päästä kaikille halukkaille. Myös sen muut ominaisuudet ovat hieman puutteellisia. Nykyään kaivataan parempaa tukea muun muassa mobiililaitteille, palvelun laadulle ja tietoturvalle. Tulevaisuudessa Internet Protokollan version 6 odotetaan korvaavan IPv4:n kokonaan ja seuraavassa alaluvussa esittelenkin IPv6:n.

4.3 IPv6

Internet Protokollan version neljä korvaajaksi on kehitetty versio kuusi (IPv6). Sen uusia ominaisuuksia verrattuna neljänteen versioon ovat laajempi osoiteavaruus, tietoturva ja 64-bittiseen arkkitehtuuriin perustuva yksinkertaistettu rakenne, joka perustuu pääotsikkoon ja lisäotsikoihin. [25]

4.3.1 Rakenne



Kuva 4.10: IPv6:n pakollinen otsikko [50], [25]

IPv6:n pääotsikko on esitetty kuvassa 4.10. Sen kenttien nimet selittävät hyvin niiden käyttötarkoituksen. Pääotsikon yhteispituus on 320 bittiä ja sen on mahdollista olla ainoa IPv6:n otsikko paketissa.

***Versio* (engl.*Version*)**

Versio tarkoittaa versionumeroa eli kuusi tässä tapauksessa.

***Vuontunniste* (engl. *Flow Label*)**

Vuontunnisteen avulla paketit voidaan jakaa loogisiin ryhmiin.

***Luokkakenttää* (engl. *Traffic Class*)**

Luokkakenttää voidaan käyttää vuontunnisteen lisäksi luokitteluun.

***Kuorman pituus* (engl. *Payload Length*)**

Kuorman pituus tarkoittaa pakollisen pääotsikon jälkeisen IPv6-paketin osaa. Sen pituus ilmoitetaan oktetteina.

***Seuraava otsikko* (engl. *Next Header*)**

Seuraava otsikko -kentällä ilmoitetaan seuraavana tuleva lisäotsikko tai ylempi protokolla.

***Elinikä* (engl. *Hop Limit*)**

Elinikä vastaa IPv4:n TTL-kenttää ja ilmoittaa paketin eliniän hypyissä.

***Lähde- ja kohdeosoite* (engl. *Source and Destination Address*)**

Viimeisenä pääotsikossa ovat *lähde- ja kohdeosoitteet*, joista kerrotaan enemmän seuraavassa alaluvussa.

IPv6:n rakenne perustuu pääotsikon ja lisäotsikoiden ketjutukseen. Pääotsikolla tuotetaan peruspalvelut kuten kuljetus, reititys ja pakettien luokittelu. Muiden palveluiden toteuttaminen tapahtuu ketjuttamalla pääotsikon perään lisäotsikoita. Lisäotsikot seuraavat pääotsikkoa yleensä seuraavassa järjestyksessä [50]:

- Hyppyoptio-otsikko (engl. *Hop-by-Hop Options Header*),
- Kohdeoptio-otsikko (engl. *Destination Options Header*),
- Reititysotsikko (engl. *Routing Header*),
- Lohkomisotsikko (engl. *Fragment Header*),
- Todennusotsikko (engl. *Authentication Header*),
- Salausotsikko (engl. *Encapsulating Security Payload Header*) ja
- Kohdeoptio-otsikko (engl. *Destination Options Header*).

Lisäotsikot ovat valinnaisia ja mikä tahansa edellisistä voi puuttua. Ylemmän protokollakerroksen kehys tulee viimeisen lisäotsikon jälkeen. Tärkeimmät otsikot tietoturvan ja tämän tutkielman kannalta ovat *todennusotsikko* ja *salausotsikko*. Niitä käsitellään IPSecin yhteydessä luvussa viisi.

4.3.2 Osoitteet

IPv4:n kohdalla todettiin osoitteiden riittämättömyys ja IPv6:ssa onkin korjattu asia kasvattamalla osoitteiden pituus 128 bittiin (likimäärin $3,4 * 10^{38}$ kappaletta). Osoitteiden lukumäärä on riittävä pitkän aikaa, vaikka tarpeet kasvaisivatkin. Määrää voidaan verrata maapallon pinta-alaan, joka on merialueet mukaan luettuna noin $5,1 * 10^{14} m^2$. Osoitteita riittää siis esimerkiksi jokaiselle neliösenttimetrille useampia. [50]

IPv6-osoitteet esitetään heksadesimaalimuodossa $x : x : x : x : x : x : x : x$, jossa kukin x on 16-bittinen heksadesimaaliluku. Osoitteiden muistaminen on siis huomattavasti vaikeampaa kuin IPv4:n tapauksessa. Esimerkiksi osoite $1080 : BAD8 : 2008 : 0 : 0 : 0 : FF01 : 800$ voisi olla IPv6-osoite. Sama osoite voidaan esittää myös muodossa $1080 : BAD8 : 2008 :: FF01 : 800$ lyhentämällä peräkkäiset nollat kahdella peräkkäisellä kaksoispisteellä. Kahta peräkkäistä kaksoispistettä saa käyttää vain kerran osoitteessa. [50]

IPv6-osoitteet voidaan jakaa unicast-, multicast-, ja anycast-osoitteisiin. Näiden rakenteisiin ei tutustuta tässä tutkielmassa, koska niiden rakenteella ei ole merkitystä myöhemmin esitettyihin ratkaisuihin. Ne on esitetty lähteessä [50].

4.3.3 Tietoturva

Luvussa 4.2.4 esitettiin tietoturvaongelmia, joita IPv4:ssä esiintyy. Näistä nauhoitushyökkäys, lähdeosoitteen väärentäminen ja pakettien muuntaminen voidaan estää IPv6:n lisäotsikoita (todennus- ja salausotsikko) käyttämällä. Lisäksi paketin salaaminen salausotsikolla minimoi verkon kuuntelun edut. *Internet Key Exchange* (IKE) huolehtii salaus- ja todennusotsikon tarvitsemien avainten hallinnasta. Salausotsikon ja todennusotsikon tarjoamista palveluista ja avaintenhallinnasta kerrotaan tarkemmin luvussa viisi.

4.3.4 Tulevaisuus

IPv4:n korvaaminen IPv6:lla on lähtenyt erittäin takkuisesti käyntiin, koska sen käyttöönotto edellyttää kaikkien samassa verkkosegmentissä olevien laitteiden yhtäaikaista muuttoa IPv6:een. Myös IPv4-IPv6 -siltojen tarve vaikeuttaa IPv6:een siirtymistä. Osoitteiden tarve tulee kuitenkin kasvamaan jossain vaiheessa niin suureksi, että IPv6:n käyttöönotto on ainoa vaihtoehto. Nykyiset tilapäisratkaisut IPv4:lle eivät ole kestävää kehitystä ja niiden käyttö hankaloittaa joidenkin sovellusten käyttöä.

4.4 IP-reititys

IP-pakettien välitys tapahtuu kahden laitteen välillä hyppy kerrallaan. Kukin reititin on kiinnostunut vain seuraavasta suunnasta, johon välitettävä paketti on menossa. Jotta reitittimet tietäisivät mihin suuntaan paketteja täytyy välittää, täytyy niissä olla reititystietoja. Reititystiedot tallennetaan reititystauluihin ja näitä tietoja vaihdetaan ja hankitaan reititysprotokollien avulla esimerkiksi kommunikoimalla lähimmän reitittimen kanssa. Reititysprotokollia ovat mm. *Border Gateway Protocol* (BGP), *Open Shortest Path First* (OSPF) ja *Routing Information Protocol* (RIP). [50]

Reititys tarkoittaa mekanismia, jolla paketti ohjataan lähettäjältä vastaanottajalle kohdeosoitteen perusteella. Reititys voidaan jakaa kahteen osa-alueeseen. Ensimmäinen osa-alue on paketin ohjaaminen sisääntuloliitännästä oikeaan ulostuloliitäntään (engl. *forwarding*) ja toinen on reititystaulutietojen vaihtaminen (engl. *routing*) muiden reitittimien kanssa. Reitittimet ovat siis laitteita, jotka ohjaavat paketteja kohti oikeaa kohdeosoitetta. Tässä tutkielmassa ei mennä syvemmälle reitityksen toteutukseen.

4.5 Verkonhallinta

Verkot ovat nykyisin tulleet monille organisaatioille korvaamattomiksi. Organisaatioiden verkot ovat usein suuria ja laajaa verkkoa on hankala hallita pelkästään ihmisvoimin. Tätä varten on kehitetty verkonhallintajärjestelmät. Verkonhallinnalla on tärkeä osa verkon tarjoamien palvelujen varmistajana. Hallintayhteyksien luotettavuus on puolestaan toimivan verkonhallinnan vaatimus. [41]

4.5.1 Verkonhallinnan osa-alueet

Verkonhallinta jakautuu seuraaviin osa-alueisiin ISO:n määrittelyn mukaan [79]:

1. *Vikojen hallinta* (engl. *Fault management*)
2. *Käytön hallinta* (engl. *Accounting management*)
3. *Kokoonpanon hallinta* (engl. *Configuration management*)
4. *Suorituskyvyn hallinta* (engl. *Performance management*)
5. *Turvallisuuden hallinta* (engl. *Security management*)

Nämä osa-alueet voidaan vielä jakaa kahteen osaan [41]: *verkon valvontaan* ja *verkon hallintaan*. Verkon valvontaan kuuluu suorituskyvyn, vikojen ja käytön valvonta. Valvonta on vain tietojen hakua sekä analysointia Verkon hallintaa puolestaan ovat kokoonpanon ja turvallisuuden hallinta asetuksia ylläpitämällä. [79]

Turvallisuuden hallinta

Turvallisuuden hallinta on tiedon suojelemista ja pääsynvalvontaa. Tämä sisältää salausavainten, salasanojen ja muiden pääsynvalvontakeinojen hallinnan. Erilaiset lokit, NIDS:it ja palomuurit ovat tärkeä osa turvallisuuden hallintaa. Suojeltaviin tietoihin kuuluu muun muassa informaatio verkon laitteista ja laskutuksesta. [79], [41]

Standardeja

Verkonhallinnan toteuttamiseksi tarvitaan standardeja, jotta eri valmistajien laitteista koostuvaa verkkoa saataisiin hallittua. *Simple Network Management Protocol* (SNMP) on tällainen standardi. SNMP versio 3 (SNMPv3) on uusin SNMP:n versio ja siinä on jo mukana tietoturvaominaisuuksia, joista voi lukea lähteestä [79]. SNMP on käytetyin protokolla verkonhallinnassa ja siitä on kirjoitettu jo tarpeeksi, joten protokollan ominaisuuksista en kerro tässä tutkielmassa enempää. *Common Management Information Protocol* (CMIP) on ISO:n OSI-mallin mukainen SNMP:a vastaava hallintaprotokolla. CMIP:a ei käsitellä tässä tutkielmassa enempää. [41]

International Telecommunication Union (ITU) on julkaissut standartointisektorinsa (ITU-T) toimesta suosituksen yleisille arkkitehtuurivaatimuksille telehallintaverkossa (engl. *Telecommunications Management Network*, TMN). TMN:n tarkoituksena on tarjota perusrakenne tietoliikenneverkkojen ja -palveluiden hallintaan. [81]

4.5.2 Verkonhallintajärjestelmät

Verkonhallintajärjestelmä kokoaa yhteen sovelluksia, joiden avulla hoidetaan eri tehtäviä verkonhallinnassa, ja tarjoaa niille yhtenäisen käyttöliittymän. Tavoitteena on, että liittymästä voitaisiin hoitaa kaikki verkonhallintaan liittyvät tehtävät.

Verkonhallintajärjestelmä tulee toteuttaa siten, että se näyttää hallittavan verkon yhtenä kokonaisuutena ja loogisina osina. Hallintajärjestelmä kerää tietoa verkon toiminnasta ja voi sen avulla ohjata esimerkiksi liikennettä ruuhkaisilta väleiltä vähemmän käytetyille yhteyksille.

Verkonhallintajärjestelmien toteutukselle ei ole mitään tiettyjä sääntöjä. Järjestelmiä rakennetaan yleensä tapauskohtaisesti. Järjestelmissä on kuitenkin seuraavia peruskomponentteja ja ominaisuuksia [41]:

- Graafinen käyttöliittymä, joka tarjoaa näkymän verkkoon.
- Tietokanta, johon voidaan tallentaa järjestelmän tarvitsemia tietoja.
- Tiedon keruu verkon laitteilta.
- Laajennettavuus ja muokattavuus tarpeiden mukaan.
- Ongelmien hallinta.

World Wide Web (WWW) ja verkonhallintajärjestelmät

WWW-pohjaiset käyttöliittymät hallintajärjestelmiin ovat käteviä, koska niiden avulla verkkoa voidaan hallita mistä päin tahansa Internetiä. Hallinnoijan ei enää tarvitse päivystää työpaikalla vaan verkkoa voi hallita myös kotoa verkkoyhteyden päästä.

Myös verkon käyttäjille alkaa pikkuhiljaa tulla palveluita, joissa he voivat muuttaa oman yhteytensä ominaisuuksia lähes reaaliaikaisesti asiakkaille tarkoitetun WWW-palvelun avulla. Tämä palvelu on asiakkaan liityntä palvelun tarjoajan verkonhallintajärjestelmään. Tietoturvan kannalta on haastavaa suojata tällainen järjestelmä. Ominaisuuksia, joita asiakas pääsee muuttamaan, ovat esimerkiksi yhteyden kapasiteetti ja liikenteen prioriteetti palveluntarjoajan verkossa [85].

Distributed Management Task Force (DMTF) on koonnut yhteen WWW-pohjaiselle hallinnalle tarjottavia standardeja *Web-Based Enterprise Management* (WBEM) -nimen alle. WBEM sisältää muun muassa yleisen tietomallin, tiedon koodausmallin ja kuljetusmekanismin tiedolle. [86]

5 IPSec

Edellisessä luvussa todettiin IPv4:llä olevan tietoturvaongelmia. Eräänä ratkaisuna tietoturvaan on *Internet Protocol Security* (IPSec). IPSec on internetin turvallisuusprotokollaperhe. Se mahdollistaa turvallisen kommunikoinnin eri laitteiden välillä. Sillä voidaan suojata esimerkiksi työasemien, turvallisuusyhdyskäytävien[6] ja etätyöasemien välinen liikenne.

IPSec ei ole mikään uusi asia vaan sen kehitys on lähtenyt alkuun vuonna 1992 ja *Internet Engineering Task Forcen* (IETF) IPSec-työryhmä on perustettu 1993 [56]. Kunnolla kehitys pääsi vauhtiin IPv6:n kehitystyön myötä. IETF julkaisi RFC-dokumenttisarjassaan IPSecin 1995. Nykyinen versio, jota käsitellään tässä tutkielmassa, on julkaistu vuonna 1998 samassa IETF:n dokumenttisarjassa. Silloin uutena tuli mukaan *Internet Key Exchange* (IKE) -avaintenhallintaprotokolla. IKE ei ole ainoa avaintenhallintaprotokolla IPSecille, mutta se on tullut suosituimmaksi, koska se on valittu kiinteäksi osaksi IPSec-standardia. [82]

5.1 IPSecin palvelut

IPSecin salaus- ja autentikointiprotokollat toimivat verkkokerroksella (IP-kerros) eli sen avulla on mahdollista salata kaikki IP:n yläpuolella kulkevat protokollat kuten *Transmission Control Protocol* (TCP) ja *User Datagram Protocol* (UDP). Lisäksi, ehkä tärkeimpänä ominaisuutena, se toimii läpinäkyvästi käyttäjän ja sovelluksen kannalta eli niiden ei tarvitse huomioida IPSeciä mitenkään. IPSec on saatavilla lähes kaikkiin IPv4-toteutuksiin laajennuksena ja se on osa IPv6:sta. [8]

IPSecin tarjoamat palvelut ovat [8]

- pääsynvalvonta,
- luottamuksellisuus,
- eheystarkistus,
- todennus,

[6] Turvallisuusyhdyskäytävä nimitystä käytetään tässä tutkielmassa laitteesta, joka toteuttaa IPSecin ja välittää liikennettä eteenpäin. Tällaisia laitteita ovat esimerkiksi IPSecin toteuttavat palomuurit ja reitittimet.

- suoja nauhoitushyökkäyksiä vastaan,
- tuki IP-pakkauksen neuvottelulle ja
- rajoitettu suoja liikenteen analysointia vastaan.

Näitä palveluita hyödyntämällä pystytään estämään jo edellä mainittujen lisäksi osoitehuijaukset ja yhteyksien kaappaamiset.

5.2 IPSecin arkkitehtuuri

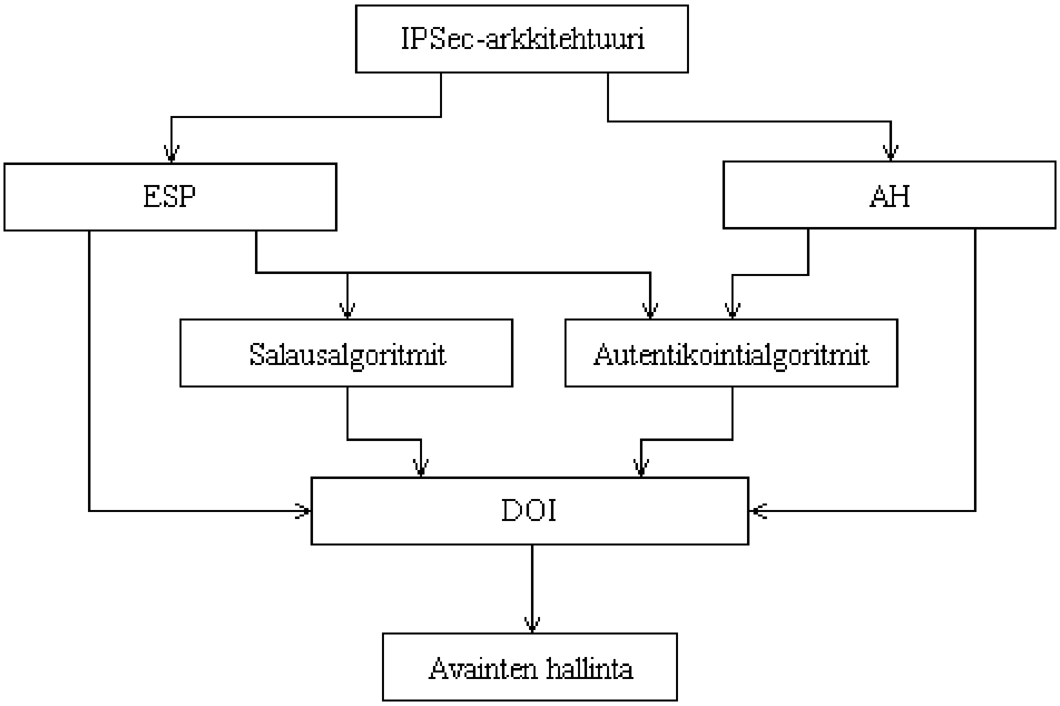
IPSec käyttää kolmea protokollaa toteuttaakseen tietoliikenteen turvallisuuspalvelut – *todennusotsikko* (engl. *Authentication Header*, AH), *salausotsikko* (engl. *Encapsulating Security Payload*, ESP) ja *IKE-avaintenhallintaprotokolla*.

IPSec perustuu yhteydettömään tilalliseen periaatteeseen. IP-paketit jaetaan luokkiin, jotka saavat erilaisen turvallisuuskohtelun. Tätä kutsutaan IPSec-politiikaksi. Politiikka voi esimerkiksi määrätä, että kaikki telnet-liikenne täytyy salata ESP:lla käyttäen 3DES-algoritmia ja todentaa käyttämällä HMAC-mekanismia SHA-1 -algoritmilla. [82]

5.2.1 IPSecin dokumentointi

IPSeciä kehitetään IETF:n IP Security Protocol -työryhmässä ja sen kotisivulta [48] löytyy kaikki IPSecin voimassaolevat RFC-dokumentit. Niissä on sekä tiedotteita että teknisiä dokumentteja. Dokumenttien väliset suhteet on kuvattu lähteessä [28] ja ne esitetään kuvassa 5.11.

IPSec arkkitehtuuri -dokumentit kuvaa IPSeciä yleisesti. ESP- ja AH-dokumenteissa kuvataan kyseiset protokollat. Niistä esitetään esimerkiksi kehysrakenteet ja oletusarvot. Salausalgoritmidokumenteissa kuvataan ESP:n kanssa käytettävät salausalgoritmit ja vastaavasti todennusalgoritmit kuvataan omissa dokumenteissaan. Todennusalgoritmeja käytetään sekä AH:n että ESP:n kanssa. Avaintenhallintadokumenteissa, jotka näkyvät kuvassa pohjalla, kuvataan luonnollisesti avaintenhallintaan liittyviä asioita kuten IKE ja *Internet Security Association and Key Management Protocol* (ISAKMP). IPSec *Domain Of Interpretation* (DOI) -dokumenteissa kerrotaan miten eri dokumenteissa olevat asiat liitetään toisiinsa. Tämä sisältää esimer-



Kuva 5.11: IPSecin dokumenttien rakenne [28]

kiksi todennusalgoritmien liittämisen avaintenvaihtoprotokollaan. IPSec on pyritty siis tekemään modulaariseksi, jotta siihen olisi helppo lisätä esimerkiksi erilaisia salaus- tai todennusalgoritmeja. [28]

5.2.2 IPSecin toimintamoodit

IPSeciä voidaan käyttää eri moodeissa käyttötarkoituksen mukaan. Turvallisuusyhdyskäytävien välillä käytetään tunnelintimoodia, jossa IP-paketti kapseloidaan kokonaisuudessaan uuteen IP-pakettiin. Kuljetusmoodissa lisätään vain tarvittavat otsikkokentät (AH ja/tai ESP) ja se suojaa siten pääasiassa IP:tä ylempiä protokollakerroksia. Kuljetusmoodia ei voida käyttää kuin IP-pakettien lopullisten vastaanottajien välillä. Tunnelointimoodin etuna on, että se piilottaa alkuperäisen IP-kehyksen tiedot lähettäjästä ja vastaanottajasta. Tunnelointimoodin käyttö vaikeuttaa siis liikenteen analysointia. Tunnelointimoodia voidaan käyttää myös yhteyden päätepisteiden välillä turvallisuusyhdyskäytävien lisäksi.

5.3 Authentication Header (AH)

Todennusotsikko (engl. *Authentication Header*, AH) on IPSecin protokolla. Sen ominaisuuksiin kuuluu yhteydetön paketin eheyden tarkistaminen ja alkuperän todennus. AH tarjoaa myös suojan vastaushyökkäyksiin (nauhoitushyökkäyksiin). Tämä tarkoittaa, että matkalla kaapattuja paketteja ei voida käyttää hyökkäyksiin lähettämällä niitä uudelleen, koska paketit yksilöidään *järjestysnumerolla*. Tämä toteutuu vain, jos vastaanottaja tarkistaa järjestysnumeron. *Internet Assigned Numbers Authority* (IANA) on kiinnittänyt AH:n protokollanumeroksi 51:n ja sitä käytetään AH:n tunnistamiseen sekä IPv4:ssa että IPv6:ssa edellisen otsikon *seuraava otsikko* -kentässä. [6], [46]

5.3.1 Todennusotsikon rakenne

Todennusotsikon rakenne on samanlainen sekä IPv4:ssä että IPv6:ssa. Todennusotsikko ketjutetaan IPv6:ssa muiden lisäotsikoiden tapaan. Seuraavaksi selitän kuvassa 5.12 näkyvien kenttien merkityksen. [6]

0	8	16 ... 31
Seuraava otsikko	*Pituus*	*Varattu*
Security Parameters Index (SPI)		
Järjestysnumero		
Autentikointidata (vaihtuvan mittainen)		

Kuva 5.12: Todennusotsikon rakenne

Seuraava otsikko

Seuraava otsikko on 8 bitin pituinen kenttä, joka ilmaisee seuraavan otsikon tai muun kuorman tyypin. Tyyppinumeroiden määrittelystä huolehtii IANA.

Pituus

Pituus-kenttä on myös 8 bittinen. Se määrittelee AH:n pituuden 32 bittisinä sanoina vähennettynä kahdella. Kahden vähennys johtuu IPv6:n lisäotsikoiden määrittelystä.

Varattu

Tämä 16 bittinen kenttä on varattu tulevaisuutta varten. *Varattu*-kenttä täytyy asettaa nollaksi toteutuksissa.

Security Parameters Index (SPI)

SPI eli *turvallisuusindeksi* on keinotekoinen 32 bittinen arvo, joka yksilöi *turvayhteydet* (engl. *Security Association*, SA).

Järjestysnumero

Järjestysnumero on 32 bittinen automaattisesti kasvava laskuri. Se on pakollinen ja aina läsnä, vaikka vastaanottaja ei käyttäisikään vastauksenestoa.

Autentikointidata

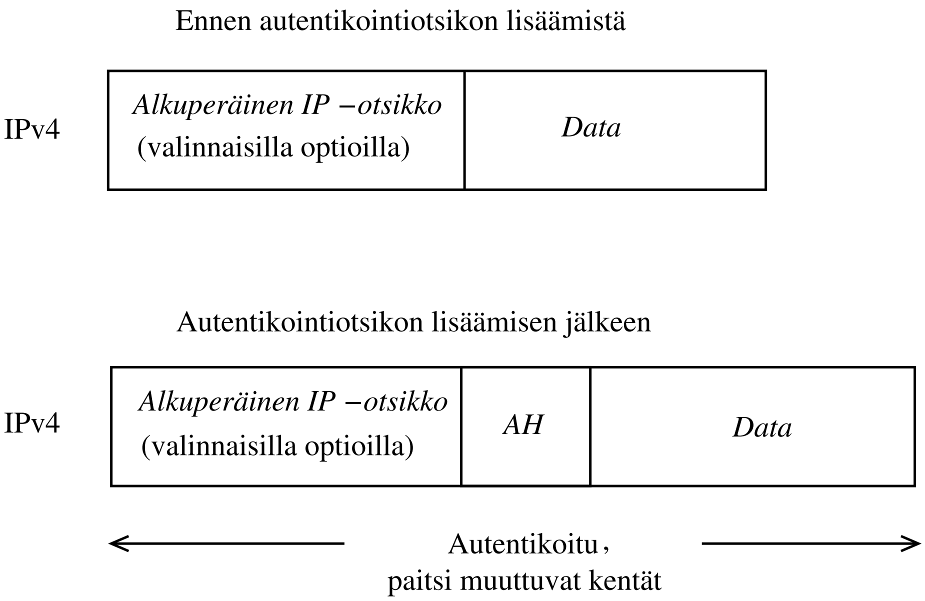
Vaihtelevanmittainen, normaalisti 96 bittinen, kenttä sisältää kryptografisen summan (engl. *Integrity Check Value*, ICV). Sen avulla voidaan tarkistaa paketin eheys ja todentaa lähettäjä. *Autentikointidata* lasketaan koko IP-paketista (lukuun ottamatta muuttuvia kenttiä) esimerkiksi luvussa kolme esitetyn HMAC-mekanismin avulla. Kentän pituuden täytyy olla IPv4:ssä 32 bitin monikerta ja IPv6:ssa 64 bitin monikerta. Tarvittaessa loppu täytetään täytteellä, jolloin pituudeksi muodostuu 32 bitin tai 64 bitin monikerta.

5.3.2 Todennusotsikon sijainti IP-paketissa

Todennusotsikon sijoittautuminen eri moodeissa ja eri IP:n versioilla näkyy seuraavista kuvista 5.13, 5.14, 5.15 ja 5.16.

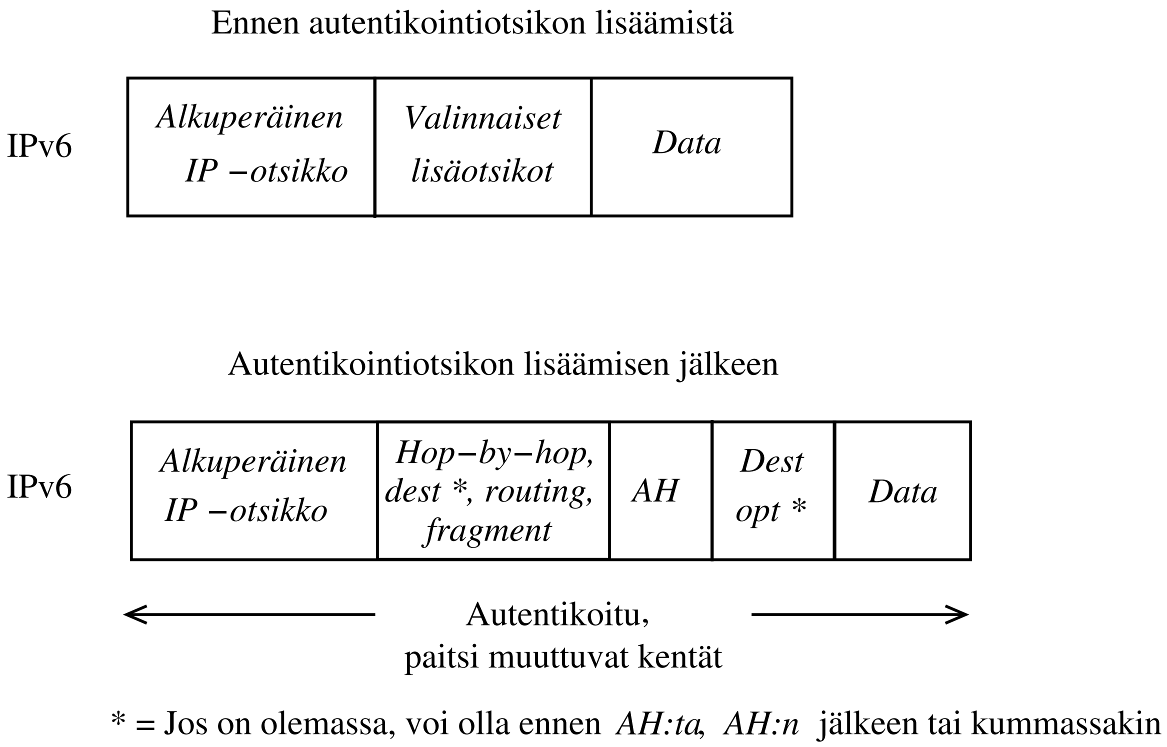
Kuljetusmoodi

AH-otsikko sijoitetaan kuljetusmoodissa IPv4:ä käytettäessä *alkuperäisen IP-otsikon* ja *datan* väliin kuvan 5.13 mukaisesti. Kuvassa 5.13 näkyy myös, että IPv4:n tapauksessa *autentikointidata* ja *alkuperäinen IP-otsikko* otetaan huomioon kryptografista tarkistussummaa laskettaessa. Muuttuvia kenttiä ei kuitenkaan oteta huomioon laskettaessa kryptografista tarkistussummaa. Tällaisia kenttiä ovat TTL, liput, TOS, fragment offset ja otsikon tarkistussumma. Myös kohdeosoite voi olla muuttuva, mutta se on ennustettavissa, joten se otetaan mukaan autentikointidataa laskettaessa.



Kuva 5.13: Autentikointiotsikon sijainti IPv4 kuljetusmoodissa

Kuvassa 5.14 näkyy, että IPv6:n tapauksessa *autentikointidata* kattaa koko IP-paketin lukuun ottamatta muuttuvia kenttiä kuten IPv4:nkin tapauksessa. Muuttuvia kenttiä IPv6:ssa ovat luokkakenttä, vuon tunniste ja elinikä. Myös kohdeosoite voi olla muuttuva, mutta se on ennustettavissa, joten se otetaan mukaan autentikointidataa laskettaessa. AH-otsikko sijoitetaan IPv6:n tapauksessa *alkuperäisen IP-otsikon* ja kuljetuksessa tarvittavien lisäotsikoiden jälkeen. *Dest opt* -lisäotsikko voi olla joko ennen AH:ta tai sen jälkeen.



Kuva 5.14: Autentikointiotsikon sijainti IPv6 kuljetusmoodissa

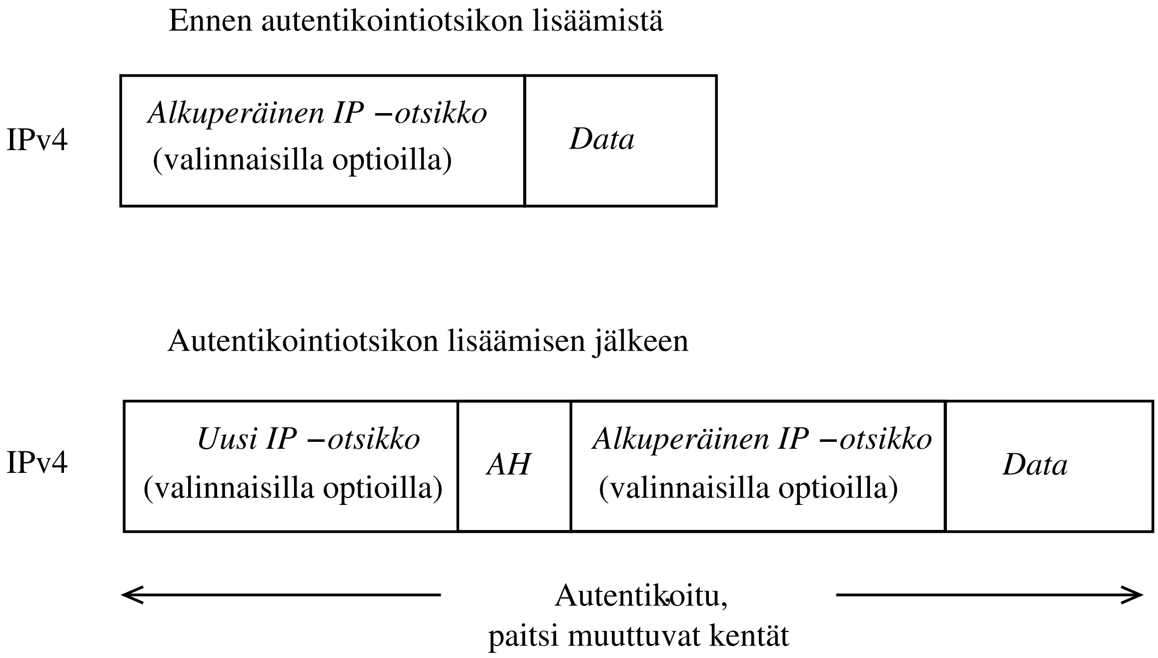
Tunnelointimoodi

AH-otsikko sijoitetaan tunnelointimoodissa IPv4:ä käytettäessä *uuden IP-otsikon* ja *alkuperäisen IP-otsikon* väliin kuvan 5.15 mukaisesti. Kuvassa 5.15 näkyy myös, että IPv4:n tapauksessa uusi IP-otsikko otetaan huomioon kryptografista tarkistussummaa laskettaessa. Muut tiedot ovat samoja kuin kuljetusmoodissa.

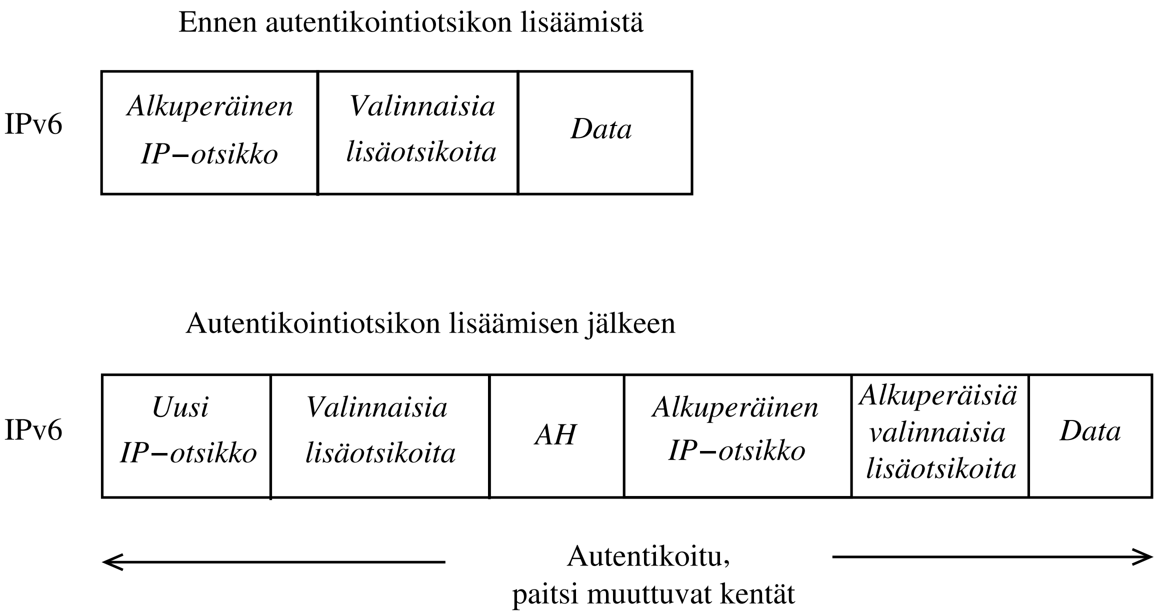
Kuvassa 5.16 näkyy, että IPv6:n tapauksessa *autentikointidata* kattaa koko IP-paketin. Tämä tarkoittaa, että muuttuvia, ennustamattomissa olevia, kenttiä lukuun ottamatta kaikki kentät otetaan huomioon tarkistussummaa laskettaessa.

5.4 Encapsulating Security Payload (ESP)

ESP on IPSecin salausprotokolla. Sen ominaisuuksia on luottamuksellisuuden takaaminen salauksella, paketin eheyden tarkistaminen ja alkuperän varmistaminen. Sen todennus ei ole aivan yhtä kattava kuin AH:ssa. Todennuksen kattavuudesta on



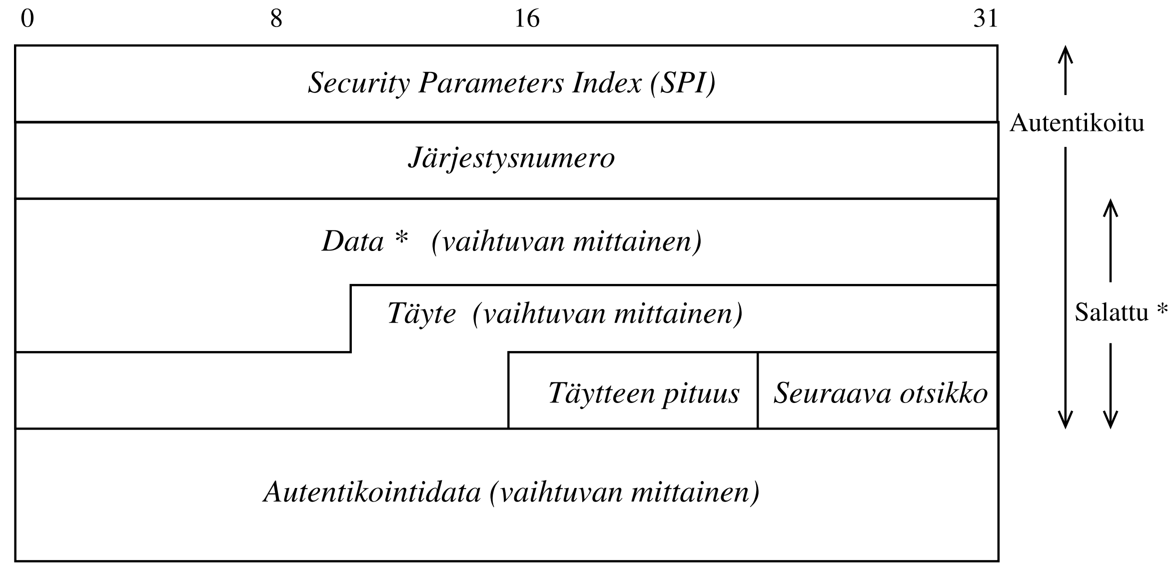
Kuva 5.15: Autentikointiotsikon sijainti IPv4 tunnelointimoodissa



Kuva 5.16: Autentikointiotsikon sijainti IPv6 tunnelointimoodissa

kerrottu enemmän alaluvussa 5.4.2.

5.4.1 ESP:n rakenne



* Jos *Initialization Vector* (IV) on mukana kuormassa, ei sitä ole aina salattu, vaikka se usein luetaankin osaksi salattua tekstiä.

Kuva 5.17: Salausotsikon rakenne

Security Parameters Index (SPI)

SPI eli *turvallisuusindeksi* on keinotekoinen 32 bittinen arvo, joka yksilöi *turvayhteydet* (engl. *Security Association*, SA).

Järjestysnumero

Järjestysnumero on 32 bittinen automaattisesti kasvava laskuri. Se on pakollinen ja aina läsnä, vaikka vastaanottaja ei käyttäisikään vastauksenestoa.

Data

Data on vaihtelevanmittainen kenttä, jonka sisältö on kuvattu *seuraava otsikko* -kentässä. Jos salausalgoritmi vaatii IV:n, synkronointidataa tai muuta sellaista, ne voidaan kuljettaa tässä kentässä.

Täyte

Useista eri syistä johtuen voidaan joutua käyttämään täytettä. Salausalgoritmi voi vaatia tietyn pituisen syötteen. ESP:n kehysrakenne vaatii myös tietyn pituuden. Täytettä voi lisätä tarpeen mukaan 0-255 tavua. *Täyte*-kenttä ei ole pakollinen, koska myös pituus nolla on mahdollinen.

Täytteen pituus

Edellisen *täyte*-kentän pituus. *Täytteen pituus* -kenttä on pakollinen, vaikka täytettä ei olisikaan.

Seuraava otsikko

Seuraava otsikko on 8 bitin pituinen kenttä, joka ilmaisee seuraavan otsikon tai muun kuorman tyypin. Tyyppinumeroiden määrittelystä huolehtii IANA.

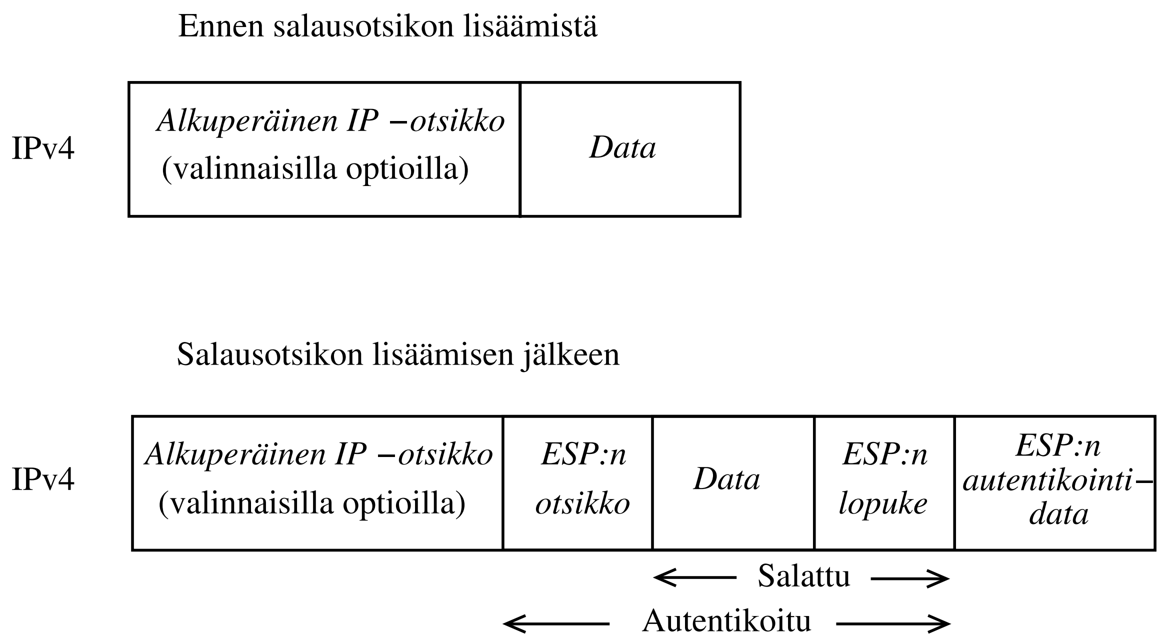
Autentikointidata

Vaihtelevanmittainen, normaalisti IPv4:n yhteydessä 96 bittinen, kenttä sisältää kryptografisen tarkistussumman (engl. *Integrity Check Value*, ICV). Sen avulla voidaan tarkistaa paketin eheys ja todentaa lähettäjä. *Autentikointidata* lasketaan koko ESP-paketista (lukuun ottamatta *autentikointidataa*) esimerkiksi luvussa kolme esitetyn HMAC-mekanismin avulla. Kentän pituuden täytyy olla IPv4:ssä 32 bitin monikerta ja IPv6:ssa 64 bitin monikerta. Tarvittaessa loppu täytetään täytteellä, jolloin pituudeksi muodotuu 32 bitin tai 64 bitin monikerta.

5.4.2 ESP:n sijainti IP-paketissa

Salausotsikon sijoittautuminen eri moodeissa ja eri IP:n versioilla näkyy seuraavista kuvista 5.18, 5.19, 5.20 ja 5.21.

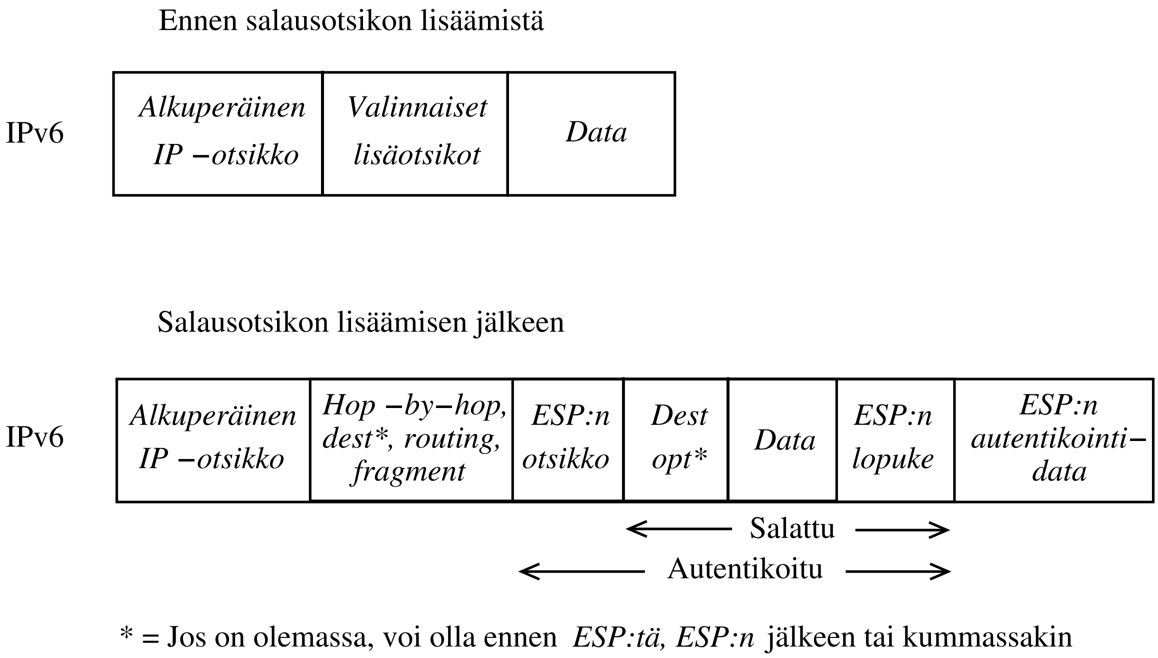
Todennuksen kattavuutta voi verrata esimerkiksi kuvien 5.18 ja 5.13 avulla. Kuvassa 5.18 näkyvässä ESP:n kuljetusmoodissa ei todennussumman laskemiseen ei oteta huomioida *autentikointidataa* eikä IP:n alkuperäistä otsikkoa. Kuvassa 5.13 puolestaan näkyy, että AH:n tapauksessa *autentikointidata* ja alkuperäinen IP-otsikko otetaan huomioon kryptografista tarkistussummaa laskettaessa. Näin on myös IPv6:n tapauksessa. Tästä seuraa, että sekä AH:n että ESP:n käyttäminen samaan pakettiin voi olla järkevää. Jos AH:a ja ESP:a käytetään samaan pakettiin, kannattaa paketti ensin salata ESP:lla ja sen jälkeen allekirjoittaa se AH:lla. Tämä tehdään näin, koska siten saadaan salatulle paketille kattavin mahdollinen todennus.



Kuva 5.18: Salausotsikon sijainti IPv4 kuljetusmoodissa

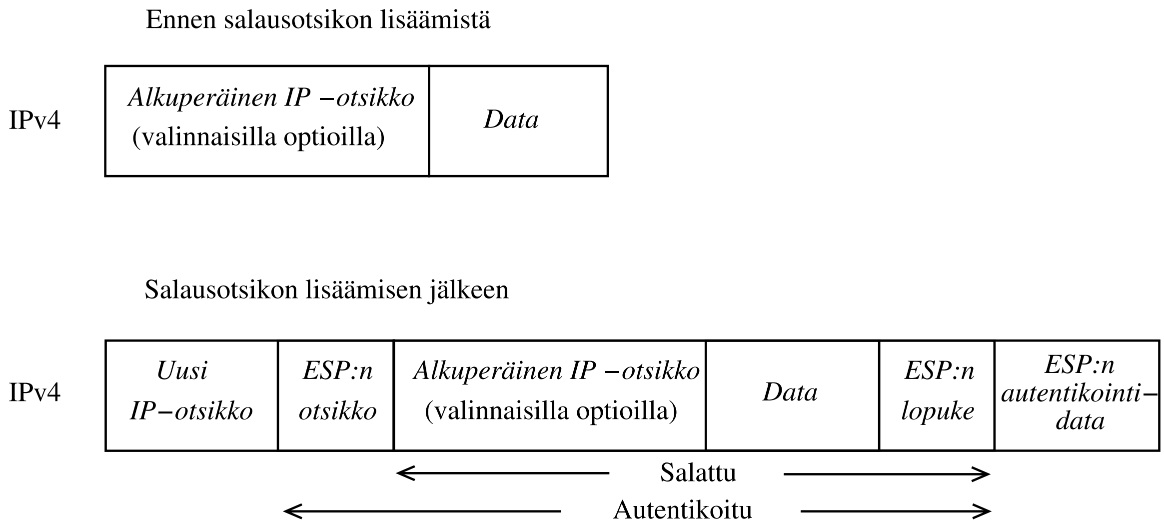
Kuvassa 5.19 näkyy ESP-lisäotsikon sijainti kuljetusmoodissa IPv6:n tapauksessa. Siinä ei ole käytännössä eroa IPv4:n tapauksen kanssa.

Kuvassa 5.20 näkyy ESP-otsikon sijainti tunnelointimoodissa IPv4:n tapauksessa. ESP:n tunnelointimoodissa on etuna kuljetusmoodiin nähden se, että alkuperäinen IP-otsikko on salattu ja todennettu. Tämä vaikeuttaa esimerkiksi liikenteen analysointia, koska lopullista määränpäätä ei pysty paketista sanomaan. Tunnelointimoodia kannattaa ESP:n tapauksessa edellisen perusteella käyttää, vaikka liikennöinti tapahtuisi kahden yksittäisen IPSec-laitteen välillä. ESP:n *autentikointidata* jää edel-

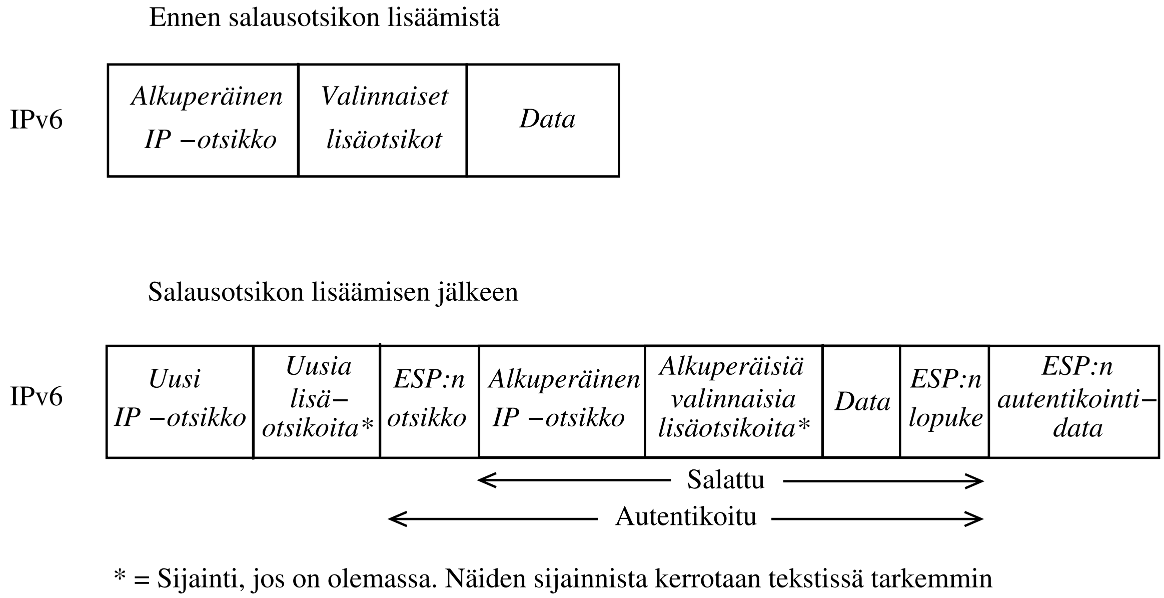


Kuva 5.19: Salausotsikon sijainti IPv6 kuljetusmoodissa

leen suojatta tunnelointimoodissa. Samoin on myös IPv6:n tapauksessa, joka näkyy kuvassa 5.21



Kuva 5.20: Salausotsikon sijainti IPv4 tunnelointimoodissa



Kuva 5.21: Salausotsikon sijainti IPv6 tunnelointimoodissa

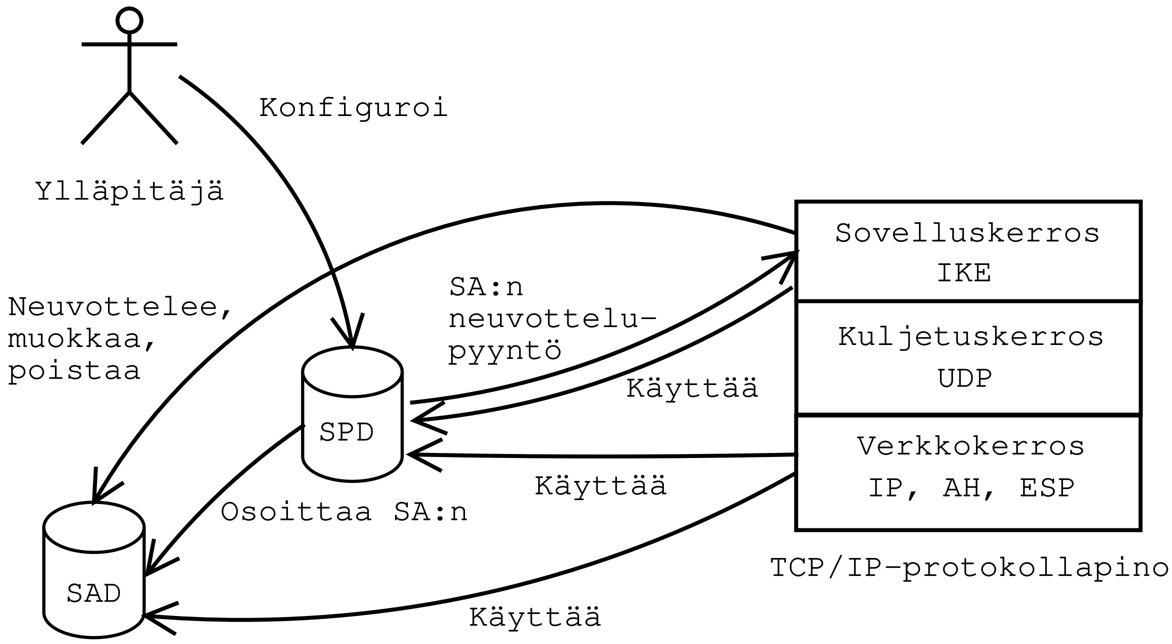
5.5 IPSecin toiminta

IPSeciä käytetään kahden IP-verkkolaitteen välisen tietoliikenteen suojaamiseen. Ennen kuin päästään vaiheeseen, jossa liikenne on suojattu halutulla tavalla, on tehtävä muutamia asioita. Ensimmäisenä ylläpitäjän on määriteltävä *turvapolitiikka* halutulle yhteydelle. Turvapolitiikat tallennetaan *turvapolitiikkatietokantaan* (engl. *Security Policy Database*, SPD). Seuraavaksi on neuvoteltava *turvayhteydet* (engl. *Security Association* (SA), jotka määrittelevät IP-pakettien käsittelyn. Todennus ja salaus vaativat salaisia avaimia. Näiden avainten vaihto on tehtävä vielä ennen kuin päästään aloittamaan itse siirto.

IP-paketin lähtiessä tarkistetaan SPD:n toimesta, mihin SA:han se kuuluu. Seuraavaksi SA:n tietojen perusteella paketin käsittelee AH ja/tai ESP. Vastaanottopäässä tutkitaan vastaavasti, mihin SA:han paketti kuuluu ja tehdään sille sen mukainen käsittely.

Kuvassa 5.22 on koottu yhteen IPSecin toimintaperiaate. Yleensä kuvassa näkyvät osat ei näy käyttäjälle erillisinä.

Jos SA:ta ei ole SPD:ssa määritellylle uloslähtevälle liikenteelle SPD pyytää IKE:a neuvottelemaan sen. Sisääntulevan liikenteen kohdalla SA:n puuttuminen merkit-



Kuva 5.22: IPSecin toiminta

see pakettien pudottamista pois. Jos paketit eivät ole IPSec-liikennettä, ne voidaan päästää ohi tai pudottaa pois politiikan mukaisesti.

5.5.1 Turvapolitiikkatietokanta

Turvapolitiikkatietokanta (SPD) määrittelee IP-paketeille tarjottavat tietoturvapalvelut riippuen muun muassa lähde- ja kohdeosoitteesta sekä liikenteen suunnasta. SPD sisältää samankaltaisia listoja kuin palomuureissakin liikenteen käsittelylle. Siellä voidaan määritellä ettei jotain tiettyä liikennetyyppiä käsitellä IPSecin toimesta ollenkaan tai pudotetaan kokonaan pois.

5.5.2 Turvayhteydet ja niiden hallinta

IPSec *turvayhteyden* (SA) käsite on keskeinen IPSecin toiminnassa. Turvayhteyttä voi kuvata loogisena yksisuuntaisena tiedonsiirtokanavana (tunnelina). Turvayhteyden yksilöi kolme asiaa: IP-paketin kohdeosoite, turvallisuusindeksi (SPI) ja turvallisuusprotokolla (AH tai ESP). Kummallekin turvaprotokollalle on oltava omat

SA:nsa (kaksisuuntaiselle yhteydelle siis yhteensä neljä), jos molempia käytetään yhtä aikaa. [82]

SPI on 32 bittinen kokonaisluku, joka lähetetään jokaisessa AH- ja ESP-kehyksessä. SPI:n avulla pystytään erottelemaan samaan osoitteeseen samalla turvallisuusprotokollalla menevät yhteydet. IANA on varannut SPI-numerot 1-255. Nollaa käytetään vain paikallisesti toteutuskohtaisena. SPI:n valitsee yhteyden kohde turvayhteyden neuvottelussa. [18]

Turvayhteyden perusteella määritellään millainen käsittely kyseiseen yhteyteen kuuluvalle paketille tehdään. Sen perusteella selviää esimerkiksi käytettävät salaus- ja todennusalgoritmit. Turvayhteydet (SA) voi luoda manuaalisesti tai automaattisesti avaintenhallintaprotokollan avulla. Manuaalisesti luodut täytyy poistaa myös manuaalisesti. Manuaalisia yhteyksiä ei saa pitää voimassa kauaa, koska niissä käytetään samaa salausavainta koko yhteyden ajan. Saman salausavaimen käyttäminen pidempään mahdollistaa suuremman määrän analysoitavaa tietoa avaimen murtoa varten, josta kerrottiin tarkemmin alaluvussa 3.5 hyökkäyksien yhteydessä. SA:t tallennetaan *turvayhteystietokantaan* (engl. *Security Association Database*, SAD). [27]

IKE:llä on omat IKE SA:t, joista kerrotaan alaluvussa 5.6.

5.6 Avaintenhallinta

Avaintenhallinta sisältää avainten luonnin, siirron, varmistuksen, poistamisen ja päivittämisen uuteen. Tärkein tehtävä IPSecin avaintenhallinnassa on avainten sopiminen salausta ja todennusta varten. [82]

IKE on IPSecin virallinen avaintenhallintaprotokolla, mutta muitakin protokollia voidaan käyttää. Avaintenhallinta voidaan hoitaa myös manuaalisesti, josta kerron seuraavassa alaluvussa.

5.6.1 Manuaalinen avaintenhallinta

IPSecin manuaalinen avaintenhallinta toimii siten, että SA:t konfiguroidaan manuaalisesti. Tässä tapauksessa on määriteltävä itse käytettävät protokollat, algoritmit ja kryptografiset avaimet. Manuaalisen avaintenhallinan huonoja puolia ovat [82]:

- skaalautuvuus: Kun kommunikoivien laitteiden määrä kasvaa, yhteyksien hallinta vaikeutuu järjettömäksi kytkentäistä[7] IPSec-mallia käytettäessä.
- automaattisuuden puute: Jonkun täytyy ylläpitää jatkuvasti avaimia ja yhteyksiä. Tämä johtaa henkilöstökulujen kasvuun.
- avainten päivittämisen vaikeus: avaimet pitää uusia tietyin väliajoin, jotta yhteys olisi turvallinen.

Jos samalla avaimella salataan kauan, mahdollinen hyökkääjä saa paljon analysoitavaa salattua/todennettua dataa analysointia helpottamaan. Tämän vuoksi kryptografisten avainten elinikä pitää rajoittaa. Elinikä voidaan määritellä ajan lisäksi tavuina.

5.6.2 IKE:n rakenne

IKE on pääasiassa IPSecin automaattinen avaintenhallintaprotokolla. Sitä voidaan kuitenkin käyttää ilmoittamaan turvayhteyden eli SA:n käytön lopettamisesta. IKE:n avaintenvaihto perustuu Diffie-Hellman -algoritmiin. Todennuksessa voidaan käyttää etukäteen jaettua salaisuutta (engl. *pre-shared key*, PSK), RSA-salausta tai digitaalista allekirjoitusta.

IKE on hybridiprotokolla eli se on muodostettu osista aiemmin kehitettyjä protokollia. IKE:ssä käytetään käytetään osia Oakleystä [65] ja SKEME:stä [53] avaintenvaihdon perustana. Lisäksi IKE pohjautuu ISAKMP:aan [60], joka on protokollamalli turvayhteyksien hallintaan. IPSec domain of interpretation (IPSec DOI) täydentää puolestaan ISAKMP-protokollamallin aukkoja, jotta ISAKMP:n voi toteuttaa IKE:een ja yhdistää nämä muihin IPSecin osiin. [20], [82]

5.6.3 Internet Security Association and Key Management Protocol (ISAKMP)

ISAKMP on viitemalli turvayhteyksien hallintaprotokollaksi eikä sovellu sellaisenaan käytettäväksi. Sitä voidaan käyttää myös muiden tietoturva-arkkitehtuurien kuin IPSecin kanssa. ISAKMP:n määritelmän pääasiallinen sisältö on viestisyntaksin määrittely, ohjeita viestien käsittelyyn, viestien kuljetusprotokolla, kahden vaiheen malli ja viestien järjestäminen vaihtoihin. [82]

[7] Kytkentäisessä mallissa kaikki IPSec-laitteet on suoraan yhteydessä toisiinsa.

ISAKMP-viestit koostuvat otsikosta ja erilaisista hyötykuormista. Viestien rakennetta ja hyötykuormia ei kuvata tässä tutkielmassa vaan ne selviät ISAKMP:n määritelmästä [60]. Vaihto sisältää yhden tai useamman viestin lähetettynä sarjassa kommunikoivien osapuolten välillä. Jokainen vaihto tapahtuu joko vaiheessa 1 tai 2.

Vaiheet määritellään siten, että ensimmäisen vaiheen tarkoituksena on luoda turvallinen kommunikointikanava osapuolten välille ja käyttää tätä kanavaa toisessa vaiheessa lopullisen turvayhteyden luomiseen. Näitä turvayhteyksiä kutsutaan *ensimmäisen vaiheen turvayhteydeksi* (engl. *phase 1 SA*) ja *toisen vaiheen turvayhteydeksi* (engl. *phase 2 SA*). Ensimmäisen vaiheen turvayhteydellä ei ole mitään tekemistä IPSec SA:n kanssa, mutta toinen on aina IPSecin tapauksessa IPSec SA.

Viestien kuljetus tapahtuu oletuksena UDP:lla käyttäen porttia 500, mutta TCP:n käyttökin on mahdollista. ISAKMP sisältää ohjeita viestien kaksoiskappaleiden käsittelyyn, uudelleenlähetykseen ja ajastukseen.

Kryptografisia menetelmiä ei määritellä ISAKMP:ssa ollenkaan. Myös avaintenvaihto on määritelmän ulkopuolella. IKE täyttää nämä aukot.

5.6.4 IPSec domain of interpretation (IPSec DOI)

ISAKMP:sta on tehty mahdollisimman yleinen ja sen vuoksi tarvitaan IPSec yhteistoiminta-alue -dokumentti (IPSec DOI) [67] täyttämään yleistetyt alueet, jotta sitä voidaan käyttää IPSecissä. IPSec DOI määrittelee vakiot SA-hyötykuormissa. Se määrittelee myös IPSecissä vaaditut neuvoteltavat kohteet.

IPSec DOI:ssa määritellään käytettävät avaintenhallintaprotokollat, mutta IKE on toistaiseksi ainoa. IPSec DOI:ssa voidaan myös määritellä uusia kuormatyyppejä, mutta niitäkään siinä ei vielä ole määritelty.

5.6.5 IKE:n toiminta

IKE:llä on yksinkertainen päätehtävä. Se neuvottelee turvayhteydet, kun muut IPSecin osat tarvitsevat niitä. Turvallisen neuvottelun lopputuloksena on molemmissa yhteyden päissä todennetut turvayhteydet valmiina muiden IPSecin osien käyttöön. IKE:ä voidaan käyttää myös muiden protokollien kanssa, mutta silloin näille protokollille täytyy olla oma IPSec DOI -dokumenttia vastaava yhteistoimintamäärittely. [82]

Aikaisemmin ISAKMP:n kohdalla esiteltiin vaiheisiin perustuva turvayhteyksien neuvottelu. IKE:n ensimmäinen vaihe voidaan suorittaa kahdessa eri moodissa: *päämoodi* (engl. *Main mode*) ja *aggressiivinen moodi* (engl. *Aggressive mode*). Toisen vaiheen suoritusta kutsutaan nimellä *Quick-moodi* (engl. *Quick mode*). IKE:n ensimmäisen vaiheen tavoitteena on muodostaa IKE SA ja toisen IPSec SA. IKE:ssä määritellään myös kaksi muuta vaihtoa: tiedonantoviesti virheilmoituksille ja tilatiedoille sekä uuden ryhmän vaihto. Uuden ryhmän vaihto mahdollistaa uuden Diffie-Hellman -ryhmän käytön. IKE:ssä määritellyt ryhmät 1 (768 bittinen), 2 (1024 bittinen) ja 5 (1680 bittinen) ovat perinteisiä alkulukujen potenssiin korotukseen perustuvia. Ryhmät 3 (155 bittinen) ja 4 (185 bittinen) perustuvat puolestaan elliptisiin käyriin. Näistä vain ryhmä 1 on pakollinen toteuttaa standardin mukaan, mutta muiden toteutus on erittäin suositeltavaa turvallisuussyistä. Ryhmät 1 ja 3 vastaavat toisiaan vahvuudeltaan. Ryhmät 2 ja 4 ovat myös samankaltaisia keskenään. Ryhmälle 5 ei ole vielä määritelty vastinetta elliptisten käyrien puolella. [27]

Osapuolten todennus voidaan tehdä IKE:ssä seuraavin tavoin [20]:

- digitaalinen allekirjoitus,
- kaksi eri tapaa julkisen avaimen salauksella,
- etukäteen jaettu avain (engl. *pre-shared key*, psk).

Näistä vain etukäteen jaettu avain on pakollinen toteuttaa.

Main mode

Päämoodi (engl. *Main mode*) käyttää kuutta viestiä IKE SA:n muodostamiseen. Viestit on jaettu kolmeen pariin. Ensimmäisessä parissa sovitaan vaihdon suojauksesta: annetaan ehdotus tai useampia ja hyväksytään yksi. Ehdotukseen sisältyy vaiheessa 1 käytettävä salausalgoritmi, tiivistealgoritmi, todennusmenetelmä ja Diffie-Hellman -ryhmä. Tätä kutsutaan turvaehdotukseksi (engl. *protection suite*). Turvaehdotukset neuvotellaan vaihtamalla ISAKMP SA hyötykuormia. Tiivistefunktio neuvotellaan yleensä vaihdoissa, mutta sitä käytetään useimmiten HMAC-muodossa.

IKE käyttää HMAC-funktiota näennäissatunnaisena funktiona (engl. *pseudo-random function*, PRF) muodostaessaan näennäisesti satunnaista bittivirtaa. PRF voidaan antaa myös erikseen. Päämoodi on oletuksena IKE:ssä ja se on pakollinen toteuttaa. Valinnaisena voidaan antaa vaiheen 1 elinikä. Osapuolten identiteetti pysyy suojassa käytettäessä päämoodia. Neuvottelu on kuvattu taulukossa 5.5.

Suunta	Viestin hyötykuorma
A → B	SA
A ← B	SA
A → B	KE, NONCE
A ← B	KE, NONCE
A → B	ID, HASH
A ← B	ID, HASH

Taulukko 5.5: Päämoodi etukäteen jaetun avaimen todennuksella [20]

A tarkoittaa taulukossa yhteyden aloittajaa ja B vastaajaa. *Hölynpöly*[8] (engl. *NONCE*) on vain 8–256 tavua pitkä satunnaisluku, jota käytetään myöhemmin vaihtojen tuoreuden toteamiseen. Molemmilla osapuolilla on omat hölynpölynsä. Taulukon 5.5 kaksi viimeistä viestiä ovat salattuja. *Key Exchange* (KE) tarkoittaa hyötykuormaa, jossa kulkee Diffie-Hellman -avaintenneuvottelun julkiset avaimet. Viimeiset kaksi viestiä todentaa Diffie-Hellman -vaihdon. Etukäteen jaettua avainta käytetään julkisen tiedon lisäksi todennussumman (HASH) laskuun. ID on osapuolen tunniste. Edellisten hyötykuormien lisäksi viesteissä kulkee ISAKMP-otsikon mukana *eväste* (engl. *cookie*), josta ei tässä kuitenkaan enempää. Viestien sisältö eroaa hieman, kun käytetään muita todennusvaihtoehtoja. Viestit muilla todennusvaihtoehdoilla on esitetty lähteissä [20] ja [27].

Aggressive mode

Aggressiivinen moodi (engl. *Aggressive mode*) on lyhennetty versio Main modesta. Erona päämoodiin on se, että identiteetit selviää mahdolliselle salakuuntelijalle, koska

[8] Hölynpölyn tarkoituksena on tehdä viesteistä erilaisia, jotta nauhoitushyökkäyksiä ei voi tehdä. Englanniksi sitä kuvataan seuraavasti: A word occuring, invented, or used just for a particular occasion. [78]

mitään viestejä ei salata. Aggressiivinen moodi on vapaaehtoinen toteuttaa. Vaiheen 1 kulku tässä moodissa on kuvattu taulukossa 5.6. Muilla todennusmenetelmillä periaate on aivan sama ja niistä löytyy tarkat kuvaukset lähteestä [20].

Suunta	Viestin hyötykuorma
A $\rightarrow$ B	SA, KE, NONCE, ID
A $\leftarrow$ B	SA, KE, NONCE, ID, HASH
A $\rightarrow$ B	HASH

Taulukko 5.6: Aggressiinen moodi etukäteen jaetun avaimen todennuksella [20]

Kuten aikaisemmin todettiin aggressiivinen moodi on tiivistetty versio päämoodista. Siinä vaihdetaan samat tiedot kuin päämoodissa, mutta ne on laitettu vain kolmeen viestiin. Ensimmäisessä viestissä aloittaja lähettää turvaehdotuksen (SA), Diffie-Hellman -avaimen (KE), hölynpölyn (NONCE) ja oman tunnuksensa (ID). Vastapuoli valitsee omassa viestissään yhden turvaehdotuksista (SA), lähettää oman Diffie-Hellman -avaimen (KE), hölynpölyn, tunnuksensa (ID) ja todennussumman (HASH). Tähän aloittaja vastaa omalla todennussummallaan, joka kuittaa ensimmäisen vaiheen onnistuneeksi. [82]

Päämoodi on parempi hyökkäyksien kestävyydessä kuin aggressiivinen moodi, koska sen kaksi ensimmäistä viestiä ei sisällä mitään vaativia laskutoimituksia. Tämä estää useimmiten väärällä IP-osoitteella tapahtuvat hyökkäykset. Aggressiivisessa moodissa puolestaan heti ensimmäisessä vastaajan viestissä on kuluttavaa laskentaa (Diffie-Hellman avain ja todennussumma). [82]

Quick mode

Toinen vaihe on vaiheen 2 SA:n (IPSec SA) neuvottelua varten. Quick-moodi on yksinkertainen ja nopea. Se muistuttaa ensimmäisen vaiheen aggressiivista moodia. Toisen vaiheen kaikki viestit ovat suojattuja ensimmäisessä vaiheessa muodostetun IKE SA:n määrittelemällä tavalla, joten siinä ei tarvitse huolehtia osapuolten todennuksesta. [27]

Viestien vaihto on kuvattu taulukossa 5.7. Ensimmäinen viesti sisältää toisen vaiheen turvaehdotukset (SA), aloittajan hölynpölyn (NONCE) ja todennussumman

(HASH). Muut hyötykuormat ovat valinnaisia. *IDi* tarkoittaa aloittajan tunnistetta ja *IDr* vastaajan. *KE* on kuten aikaisemmin. Toinen viesti on samankaltainen kuin ensimmäinen. Se on vain vastaajan kannalta ja sisältää valitun turvaehdotuksen. Kolmas viesti kuittaa vaihdon onnistumisen ja sisältää todennussumman vaihdon tuoreuden varmistamiseksi. [82]

Suunta	Viestin hyötykuorma
A → B	HASH, SA, NONCE, [KE][9], [IDi, IDr]
A ← B	HASH, SA, NONCE, [KE], [IDi, IDr]
A → B	HASH

Taulukko 5.7: Quick mode [20]

5.7 IPSecin käyttö

IPSecin yleisin käyttötarkoitus on tällä hetkellä virtuaalisten erillisverkkojen toteutuksessa [56]. VPN:n eli virtuaalisen erillisverkon tarkoituksena on rakentaa oma turvallinen verkko julkisen (avoimen) siirtotien, esimerkiksi Internetin, yli. Perusajatuksena on estää tärkeän tiedon muuttuminen, luku ja kopiointi siirtotiellä eli taata tiedon luottamuksellisuus.

Toinen käyttötarkoitus on etäkäyttäjän tietoliikenteen suojaaminen. Etäkäyttäjä voi olla esimerkiksi langattoman verkon käyttäjä ja ottaa yhteyttä organisaation turvallisuusyhdyskäytävään.

Kolmas käyttötarkoitus IPSecille on kahden yksittäisen laitteen välisen tietoliikenteen suojaaminen. Esimerkiksi kaksi kaveria haluaa jakaa keskenään jotain luottamuksellista verkon välitykselle.

Edelliset kolme ovat IPSecin perinteisiä käyttökohteita. Uutena käyttökohteena on tietokoneiden ja verkkojen hallintayhteyksien tietoliikenteen suojaaminen IPSecillä. Tästä kerron tarkemmin luvussa kuusi.

IPSecin tarjoamaan turvaan vaikuttaa olennaisesti yhteyksissä käytetyt algoritmit ja eri käyttötarkoituksiin sopii eri algoritmit riippuen tavoitteesta. Turvallisimmat algoritmit ovat yleensä hitaimpia ja joskus on perusteltua käyttää nopeampia algoritmeja. IPSecin tukemat algoritmit esitetään seuraavissa alaluvuissa.

5.7.1 IPSecissä käytetyt salausalgoritmit

Kaikkien ESP:ssa käytettävien salausalgoritmien täytyy toimia CBC-moodissa. DES on pakollinen standardin mukaan IPSecissä ja 3DES on suositeltava vaihtoehto. Luvussa 3 todettiin, että AES-algoritmi on nopeampi kuin 3DES vastaavalla avainpituudella käytettynä. Tämän vuoksi AES tuleekin todennäköisesti syrjäyttämään tulevaisuudessa 3DES:n myös IPSecissä. AES:n käytöstä IPSecin kanssa on jo standardiluonnos [31]. IPSec standardissa on yleinen ohje [12] ESP:n kanssa käytettäville algoritmeille, jonka perusteella voi mitä tahansa CBC-moodissa toimivaa algoritmia käyttää. Toteutukset näistä algoritmeista tulevat kuitenkin usein perässä ja usein vain muutama algoritmi on toteutettu, mikä onkin järkevää selkeyden vuoksi. [27]

5.7.2 IPSecissä käytetyt todennusalgoritmit

IPSecissa käytetyt todennusalgoritmit ovat avainnettuja MAC-funktioita. Pakollisina funktioina AH:ssa, ESP:ssa ja IKE:ssä ovat HMAC-MD5 [37] ja HMAC-SHA-1 [38]. Molempia algoritmeja käytetään siten, että algoritmin tuottama tiiviste typistetään 96 bittiin. Myös HMAC-RIPEMD-160:n käytöstä on dokumentti, mutta sen toteutus ei ole pakollista. 160 tarkoittaa edellisessä tiivisteen pituutta, mutta tässäkin tapauksessa se typistetään 96 bittiin.

Uutena algoritmina todennukseen IPSecissä on tulossa SHA-2:n HMAC-versio [33], jossa 256 bittiä pitkä tiiviste typistetään 128 bittiin. Tiivisteen pituutta onkin syytä kasvattaa vähitellen, koska se parantaa kestävyyttä aikaisemmin luvussa 3 mainittuja hyökkäyksiä vastaan. Toinen tuleva algoritmi todennukseen on AES-XCBC-MAC-96 [32], joka käyttää siis nimensä mukaisesti uutta AES-salausalgoritmia kryptografisen summan muodostamiseen.

5.7.3 IPSec VPN

Eräs tapa toteuttaa VPN on käyttää IPSeciä. Muita tapoja on esimerkiksi *Multiprotocol Label Switching* (MPLS), joka soveltuu hyvin runkoverkon VPN-ratkaisuihin, ja tunnelointi *Level 2 Tunneling Protokollalla* (L2TP). IPSec sopii hyvin tapauksiin, joissa yhdistettäviä laitteita on vähän, koska IPSec VPN monimutkaistuu laitemäärän kasvaessa. Skaalautuvuutta voidaan kuitenkin parantaa käyttämällä julkisen avaimen järjestelmiä. IPSecillä voidaan toteuttaa VPN kahdella tavalla, tekemällä tunnelit kaikkien IPSec-laitteiden välille tai käyttämällä IPSec-keskitintä [10]. [2], [77]

IPSec VPN -toteutuksen hyvä puoli on sen valmistajariippumattomuus, koska se pohjautuu vapaaseen standardiin. Yritykset voivat siis käyttää siinä melko vapaasti haluamiaan laitteita, koska niiden yhteensopivuus on nykyään jo melko hyvä. IPSec VPN on myös edullinen toteuttaa pienessä mittakaavassa, koska Linux ja FreeS/WAN [36] ovat ilmaisia. IPSec VPN ei kuitenkaan sovellu hyvin suurille yhteysnopeuksille. Nykyaikainen 1,5GHz:n kellotaajuudella toimiva PC pystyy salaamaan tai purkamaan noin 50Mbit/s riippuen käytetystä algoritmista ja rautatason IPSec-salaajat ovat vielä melko kalliita. AES-algoritmin FS/WAN-toteutuksella on päästy kaksinkertaiseen nopeuteen verrattuna 3DES-algoritmiin, joten salausnopeus käytettäessä AES:a uusilla koneilla ylittää 100Mbit/s [29]. Myös aikaisemmin tässä tutkielmassa on todettu AES:n olevan 3DES:a huomattavasti nopeampi. Erilaisiin laitteisiin voi tutustua tutkimalla muun muassa SC Magazinen markkinakatsausta [19]. IPSec VPN:ssä salaus ja kapselointi aiheuttaa viivettä, josta voi olla joskus haittaa.

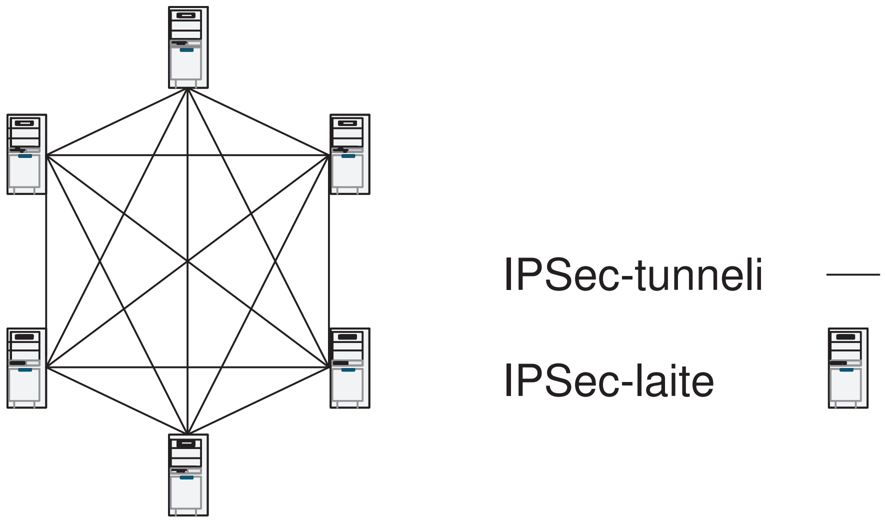
Kytkentäinen malli

Kytketyssä mallissa (kuva 5.23) kaikki IPSec-laitteet on kytketty toisiinsa suoraan IPSec-tunneleilla. Tämä on yksinkertaista kun verkossa ei ole paljon laitteita. IPSec-laitemäärän kasvaessa hallittavien VPN-yhteyksien määrä kasvaa kohtuuttomasti ja verkosta tulee vaikeasti hallittava. Ratkaisuna tähän on keskitinmalli tai tulevaisuudessa optimistinen kytketty malli, jossa yhteyksille ei tehdä asetuksia etukäteen. Keskitinmallin heikkona puolena on haavoittuvuus. Jos keskittimelle tapahtuu jotain, koko verkon salattu liikenne voi loppua. [77]

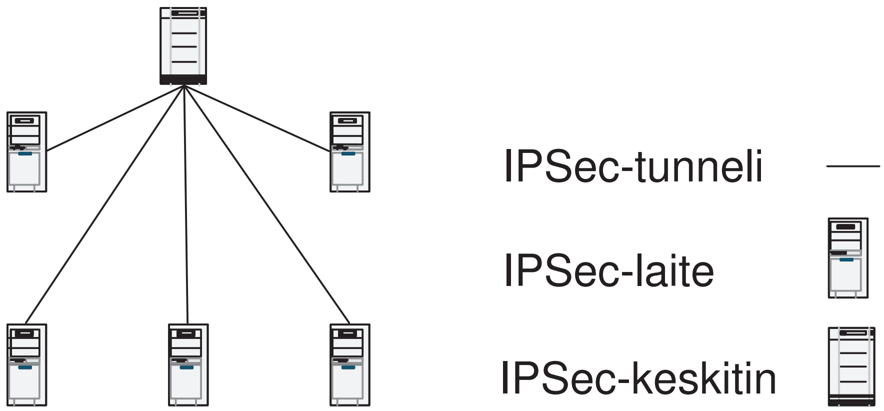
Keskitinmalli

Keskitinmallissa (katso kuva 5.24) käytössä on keskitin, jonka kautta kaikki liikenne kulkee. Muiden IPSec-laitteiden tarvitsee muodostaa tunneli vain keskittimelle,

[10] IPSec-keskittimellä tarkoitetaan tässä laitetta, jonka kautta kaikki muut IPSec-laitteet on yhteydessä toisiinsa.



Kuva 5.23: Kytkentäisen mallin looginen rakenne



Kuva 5.24: Keskitinmallin looginen rakenne

joka muodostaa yhteyden eteenpäin toiselle IPSec-päätepisteelle. Liikenne kulkee siis kahden tunnelin läpi. Keskitin joutuu ensin purkamaan ja sitten salaamaan kaiken liikenteen. Keskitinmalli vaatiikin keskittimeltä tehokkuutta, jotta se suoriutuisi kaikesta liikenteestä. Verkkokapasiteetin pitää olla myös suuri keskittimelle, koska kaikilta IPSec-laitteilta voi tulla samaan aikaan liikennettä. [77]

5.7.4 IPSecin vaikutus verkon kapasiteettiin

IPSecin käyttö laskee verkon hyötykapasiteettia, koska avainten neuvottelut vaativat useamman viestin vaihdon ja jokaisesta paketista AH ja/tai ESP vie osansa. Lisäksi tunnelointimoodia käytettäessä uusi IP-otsikko vie osansa.

IKE-neuvottelu vie ensimmäistä turvayhteyttä neuvoteltaessa noin 1650 tavua käytettäessä päämoodia ja Quick-moodia. Käytettäessä aggressiivista moodia ensimmäisessä vaiheessa säästetään hieman kapasiteettia, mutta osapuolten identiteetit paljastuvat silloin kuuntelijalle. Avainten uusiminen toisen vaiheen Quick-moodilla vie verkkokapasiteettia noin 750 tavua. [43]

Varsinaisessa käytössä ylimääräistä kapasiteettia vie IPSecin kehykset. Todennusotsikon koko on 96 bittiä ja vaihtelevanmittainen autentikointidata, joka on yleensä 96 bittiä. Salausotsikon pituus on 80 bittiä plus autentikointidata (yleensä 96 bittiä) ja mahdollinen salausalgoritmin vaatima alustusvektori (IV). Näiden lisäksi molempiin voi tulla täytettä, jotta kehykselle saadaan IPv4:n tai IPv6:n haluama pituus. Todennusotsikko ja salausotsikko siis vievät kumpikin noin 192 bittiä paketilta kapasiteettia. Jos käytetään IPSeciä tunnelointimoodissa, päälle tulee vielä uuden IP-otsikon koko (IPv4:ssä 160 bittiä ja IPv6:ssa 320 bittiä). Tunnelointimoodin käyttö siis lähes kaksinkertaistaa IPSecin kuluttaman kapasiteetin IPv4:n tapauksessa ja IPv6:n kohdalla määrä on vielä suurempi.

IPSecin aiheuttaman kuormituksen vaikutuksia on analysoitu lisää lähteessä [80], jossa on keskitytty pääasiassa suoritintehon vaikutukseen.

5.8 Yhteenveto

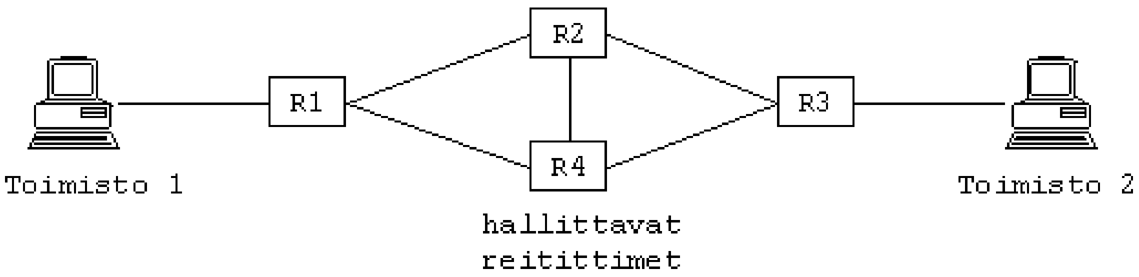
IPSec on yksi tietoturvaratkaisu TCP/IP-protokollaperheen tietoturvaongelmiin. Se ei ole kuitenkaan ainoa. Muita ratkaisuja ovat ylemmillä TCP/IP-kerroksilla toimivat protokollat, kuten esim. *Secure Shell* (SSH) ja *Transport Layer Security* (TLS) ja alemmalla eli fyysisellä tasolla toimivat salaajat. IPSec sopii kuitenkin paremmin esimerkiksi UDP-liikenteen salaamiseen kuin ylemmillä kerroksilla toimivat protokollat, koska se toimii läpinäkyvästi ylemmille kerroksille. SSH:n eduksi on kuitenkin laskettava yksinkertaisempi toteutus ja sen vuoksi se on hyvä vaihtoehto IPSecille joissakin tapauksissa. WWW-liikenteen suojaamiseen TLS on parhaiten sopiva vaihtoehto. Kuitenkin tietoturvaprotokollan valinta pitää tehdä aina tapauskohtaisesti. [64]

IPSec soveltuu moneen tarkoitukseen ja eri toteutusten yhteensopivuudet ovat melko hyviä eli IPSecin käyttöönotto ei sido yhteen laite- tai ohjelmistovalmistajaan. IPSecin kehitys on avointa ja standardi on julkaistu IETF:n toimesta, joten IPSecin tulevaisuus näyttää lupaavalta. Nyt IPSec on jo erittäin suosittu erilaisissa VPN-toteutuksissa. Laajojen IPSec-verkkojen toteutus edellyttää tehokasta hallintajärjestelmää. Käytännössä tämä tarkoittaa julkisen avaimen arkkitehtuuria varmennepalvelimella. Kaiken kaikkiaan IPSec on hyvä tietoturvaprotokollaperhe ja sen tulevaisuus on turvattu IPv6:n myötä. [56]

6 Ratkaisu verkonhallintajärjestelmän tietoliikenteen suojaamiseen

Verkon ytimen muodostavat reitittimet ja ilman niitä verkon osat eivät voi kommunikoida keskenään. On siis erittäin tärkeää varmistaa reitittimien toiminta. Reitittimien toiminnan puolesta taas verkonhallinta on keskeisessä osassa ja erityisesti turvallisuuden hallinta. Reitittimiä hallitaan useimmiten SNMP:llä tai telnet-yhteyksillä. Seuraavissa alaluvuissa esitän ratkaisun verkonhallintajärjestelmän suojaamiseen, mikä tarkentaa kehittämääni organisaation verkon tietoturvamallia.

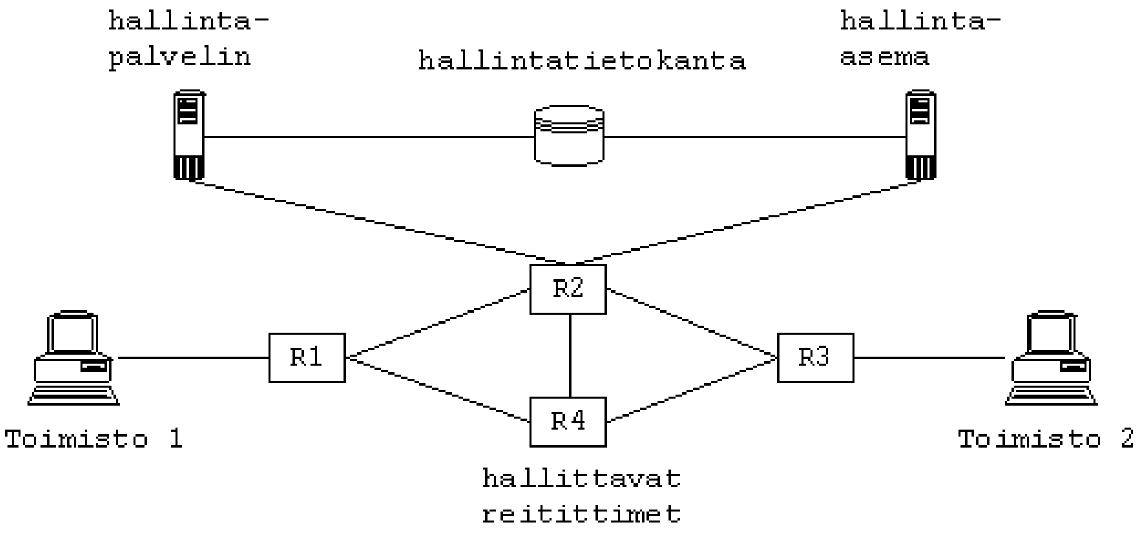
6.1 Suojaamisen kohteet



Kuva 6.25: Verkonhallinnan tavoite

Verkon komponenttien hallintayhteydet on suojattava, jotta verkko pystyy toimimaan luotettavasti. Kuvassa 6.25 on esimerkki kahden toimiston välisestä yhteydestä, jonka täytyy toimia luotettavasti tietyllä kapasiteetilla. Toimistojen välinen liikenne ohjataan tarpeen mukaan reitittimeltä 1 (R1) reitittimelle 3 (R3) joko reitittimen 2 tai 4 kautta, jotta palvelun laatu saadaan taattua. Palvelun laadun tarjoavan verkon toimintamalli on kuvassa 6.26. Kuvaan 6.26 on lisätty mukaan verkonhallintajärjestelmä (hallintapalvelin ja -asema). Malli toimii siten, että Toimisto 1 lähettää hallintapalvelimelle pyynnön esimerkiksi 1 Mbit/s yhteydestä toiselle toimistolle. Hallintapalvelin laittaa sen hallintatietokantaan pyyntöjonoon, josta hallinta-asema käy sen lukemassa. Pyynnön perusteella hallinta-asema konfiguroi reitin toimistojen välille.

Verkon käyttäjien (edellisessä toimistojen) todennus on tärkeää, jotta pystytään hallitsemaan verkon käyttöä. Verkonhallintatiedot eivät saa joutua vääriin käsiin ja nii-



Kuva 6.26: Verkonhallinnan toimintamalli

tä ei saa muokata kuin siihen valtuutetut. Näihin tietoihin kuuluu hallintatietokannat ja hallintatietoliikenne. Hallinta-asemat, -palvelin ja niiden käyttöliittymäkoneet on suojattava, koska niihin tunkeutumalla pystyy vaikuttamaan hallintaliikenteeseen. Myös hallinnan kohteet eli reitittimet on suojattava, koska muun hallinnan suojaaminen menettää merkityksensä, jos reitittimiä ei ole suojattu hyvin.

6.2 Mahdolliset uhat

Hallintajärjestelmään kohdistuvat uhat voidaan jakaa kahteen luokkaan: passiiviset ja aktiiviset. Hallintaliikenteen salakuuntelu on esimerkiksi passiivinen uhka. Kuuntelulla voidaan saada selville esimerkiksi luottamuksellia tietoja asiakkaista tai verkon rakenne. Verkon rakenteen selvittäminen on ensimmäinen asia, jonka hyökkääjä tekee. Toinen asia, jota kuuntelulla pystytään tekemään on liikenteen analysointi. Sen avulla pystytään selvittämään verkon rakennetta, vaikka liikenne olisikin salattua. Nämä hyökkäykset rikkovat liikenteen luottamuksellisuutta.

Passiivisia hyökkäyksiä on erittäin vaikea havaita, koska niissä ei puututa mitenkään pakettien liikkumiseen. Niinpä lähes ainoa keino torjua passiivisten uhkien aiheuttamia vahinkoja on suojata tieto passiivisesti, eikä niinkään yrittää havaita mahdollisia hyökkäyksiä. Aktiivinen torjuntakeino on kuitenkin olemassa. Siinä verkosta etsitään laitteita, jotka ottavat vastaan kaikki paketit eikä vain omiaan.

Aktiivisia hyökkäyksiä on kolmea luokkaa. Ensimmäisenä on pakettien muokkaaminen, jotta hyökkääjä saisi esimerkiksi muunnettua varattavan kaistan määrää tai sitä kenelle kaista varataan. Muokkaamiseen sisältyy myös vanhojen pakettien uudelleenlähetys, viivytys ja uudelleenjärjestäminen. Paketteja muokkaamalla ja vanhoja uudelleenlähettämällä voidaan suorittaa palvelunestohyökkäys, jolla pyritään saamaan järjestelmä toimintakyvyttömäksi. Toinen aktiivinen uhka on yksinkertaisesti pakettien kulun pysäyttäminen, jolloin hallintajärjestelmän toiminta pysähtyy. Kolmas hyökkäys on väärennös eli lähetetään paketteja asiakkaan tai hallintajärjestelmän nimissä. Tällä yritetään vaikuttaa järjestelmän toimintaan ja tavoitteena on esimerkiksi saada joku yhteys katkeamaan tai käyttämään pientä kaistaa. Nämä ovat vakavia hyökkäyksiä ja niitä vastaan pitää suojautua.

Aktiiviset hyökkäykset on helpompi havaita kuin passiiviset, koska niissä vaikutetaan liikkuviin paketteihin. Palvelunestohyökkäysten torjunta kokonaan on vaikeaa, koska aina voidaan olettaa, että hyökkääjällä on isompi tietoliikenne- ja konekapasiteetti käytettävissä kuin puolustettavassa järjestelmässä. Pakettien kulun pysäyttämisen estäminen esimerkiksi katkaisemalla kaapeli edellyttää jatkuvaa valvontaa ja on siten mahdotonta toteuttaa käytännössä. Aktiivisten hyökkäysten torjunta vaatii aktiivista puolustautumista passiivisen lisäksi.

Edellä mainittujen uhkien tarkkaa todennäköisyyttä on erittäin vaikea arvioida, koska niihin vaikuttaa niin monta tekijää. Se pitää arvioida tapauskohtaisesti, jolloin muuttujina on esimerkiksi organisaation julkisuus, toiminta-ala, järjestelmän laajuus ja verkon yhteys julkisiin verkkoihin. Yleisesti ottaen lähes jokaiseen yritykseen kohdistuu jonkinlainen hyökkäys vuoden aikana [1]. Hallintajärjestelmä on todennäköinen kohde vahingoittamisyrityksissä, koska sitä kautta pääsee käsiksi koko verkon toimintaan ja tuho vaikuttaa siten organisaation laajuisesti.

6.3 Kohteiden suojaaminen

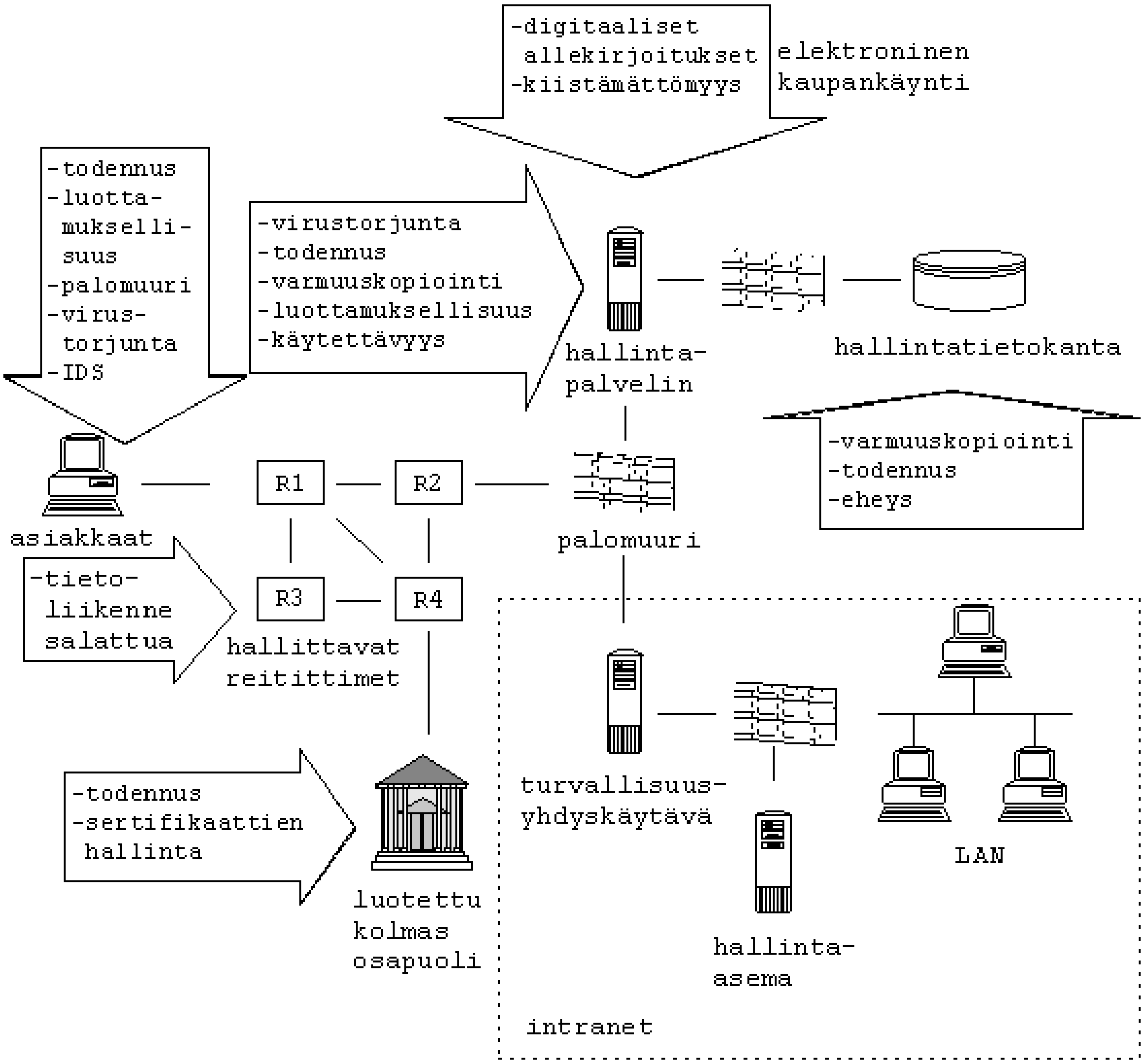
Tässä alaluvussa esitän ratkaisun uhkien torjumiseksi. Ensin on esitetty yleinen ratkaisumalli ja sitten teknologiakeskeinen ja käytännönläheinen yksittäisratkaisu, joka perustuu IPSeciin ja yleisiin tietoturvastandardeihin.

6.3.1 Yleinen ratkaisu

Alaluvussa 6.1 esitettiin verkonhallinnan toimintamalli ja suojaamisen kohteet. Niitä vastaa kuvassa 6.27 esitetyt kohteet seuraavasti. Ulkoisissa palveluissa on hallintapalvelin, joka hoitaa yhteyden käyttöliittymälle ja mahdollisten kaupallisten ominaisuuksien toteuttamisen. Hallintapalvelin käyttää tietojen tallennukseen hallintatietokantaa, joka sijaitsee tietokantapalvelimella. Asiakkailla on käyttöliittymä, joka on yhteydessä hallintapalvelimelle. Luotettu kolmas osapuoli tarkoittaa tahoa, joka varmistaa asiakkaan ja hallintapalvelimen olevan niitä, joita ne väittävät olevansa. Tämä helpottaa esimerkiksi laitteiden vaihdosta tai lisäyksestä aiheutuvia todennusongelmia, koska silloin ei osapuolten tarvitse vaihtaa sertifikaatteja esimerkiksi henkilökohtaisesti. Sisäisissä palveluissa sijaitsee varsinainen hallinta-asema. Hallinta-asema hakee pyynnöt hallintatietokannasta tietokantapalvelimelta ja tarkistaa pyyntöjen oikeellisuuden ennen kuin konfiguroi reitittimet.

Järjestelmään kohdistuvia uhkia käsiteltiin alaluvussa 6.2. Passiivisten uhkien vaikutus minimoidaan käyttämällä kryptografisia menetelmiä, vaikka hyökkäyksiä ei voidakaan yleensä havaita mitenkään. Kryptografisia menetelmiä ovat esimerkiksi salaus- ja todennusmenetelmät, joita on esitetty luvussa kolme. Salakuuntelusta ei ole hyötyä, jos pakettien sisällöstä ei saa selvää. Sen vuoksi kaikki tietoliikenne salataan. Käyttäjän todentamisella estetään hyökkääjän esiintyminen oikeana käyttäjänä eikä hyökkääjä usein pysty saamaan selville oikean käyttäjän kaikkia tietoja (kertakäyttösalasanat, käyttäjätunnukset ja sertifikaatti allekirjoitukseen). Todentaminen sisältää myös eheystarkistuksen, joten pakettien muokkaaminen havaitaan. Liikenteen analysointia ei kuitenkaan pystytä täysin estämään salauksella, mutta se mitä saadaan irti liikenteestä, on huomattavasti vähäisempää. Muun muassa antisniffer-ohjelmien avulla voi verkosta etsiä salakuuntelua tekeviä laitteita ja näin minimoida uhkia aktiivisen torjunnan avulla.

Palomuurit ovat osa passiivisten hyökkäysten torjuntaa ja niiden avulla suodatetaan tarpeeton tietoliikenne pois protokollien, porttien ja IP-osoitteiden avulla [54]. Tietokantapalvelimen ja hallinta-aseman väliin asetettavalla palomuurilla estetään muu kuin tietokannan käsittelyliikenne. Palomuureja voidaan käyttää myös aktiivisten hyökkäysten torjuntaan *Network Intrusion Detection Systemien* (NIDS) kanssa. NIDS tunnistaa jostain osoitteesta tulevan hyökkäyksen ja lisää sen palomuurin suodatuslistaan tietyksi ajaksi. Pysyväksi lisääminen ei ole hyvä juttu, koska osoitteiden



Kuva 6.27: Yleinen ratkaisu

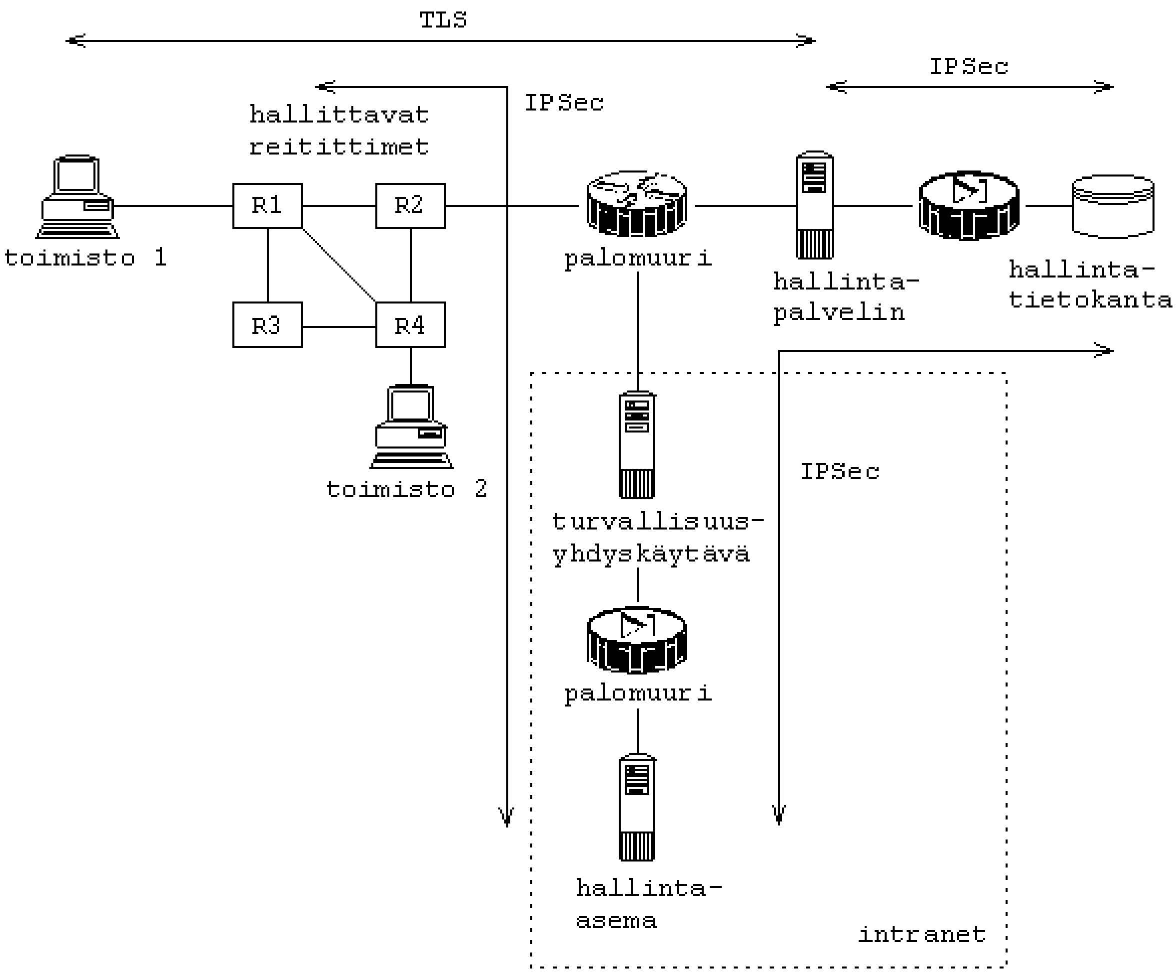
väärennös on helppoa kuten aikaisemmin tutkielman luvussa neljä todettiin. Aktiivisten palvelunestohyökkäysten torjuntaan ei ole edellisen lisäksi paljon keinoja. Yksi keino on aikaisemmin tutkielmassa mainittu pakettien merkkaus (PPM). Yleisimmin niitä vastaan varustaudutaan oman kapasiteetin lisäämisellä. Tietoliikennekapasiteettia kasvatetaan esimerkiksi kahdentamalla yhteyksiä. Hallintapalvelimia voidaan myös monistaa, jotta ne selviäisivät suuremman liikennemäärän käsittelystä ja liikenteen jakoon käytetään erilaisia tasausalgoritmeja. Haitallisten ohjelmien torjumiseksi laitteisiin asennetaan virustorjuntaohjelmat ja tärkeiden tietojen varmuuskopiointi suoritetaan säännöllisesti. Laitekohtaisia IDS:ä käytetään viimeisenä keinona havaitsemaan hyökkäys ja tiedottamaan siitä ylläpitäjälle.

6.3.2 Käytännön ratkaisu

Tässä alaluvussa esitän Terabitti-projektissa osittain käytännössä testatun ratkaisun. Ratkaisu on suunniteltu toimimaan yhdessä projektissa suunnitellun ja toteutetun verkonhallintaohjelmiston kanssa [85]. Ratkaisu ei kuitenkaan ole sidottu kyseiseen ohjelmistoon, joten siitä ei kerrota tässä. Kuvassa 6.28 esitän käytännön ratkaisun, jossa keskitytään tietoliikenteen tietoturvaan.

Asiakas käyttää omien yhteyksiensä hallintaan WWW-selainta. Selaimella otetaan yleisesti käytössä olevan *Transport Layer Security* -protokollan (TLS) [4] suojaama yhteys hallintapalvelimeen. *Secure Sockets Layer* (SSL) versio 3, joka on TLS:n edeltäjä, on todettu hyväksi antamaan suojan passiivisia hyökkäyksiä vastaan [74] ja erot SSLv3:n ja TLS:n välillä ovat hyvin pienet. Palvelimen todennukseen käytetään sertifikaatteja, jotka *varmenneviranomainen* (engl. *Certificate Authority*, CA) todentaa. Asiakkaan todennukseen käytetään kertakäyttösalasanoja käyttäjätunnuksen lisäksi. Hallintapalvelin on erotettu yleisestä verkosta palomuurilla, jotta ylimääräinen liikenne saadaan suodatettua. Vain TLS-liikenteen sallitaan kulkea läpi hallintapalvelimelle.

Hallintapalvelimelta asiakkaan pyynnöt siirtyvät tietokantapalvelimelle. Näiden palvelimien välinen liikenne on suojattu hyökkäyksiltä IPSecillä, joka salaa ja todentaa liikenteen. Tietokannan käsittelyyn tarvitaan myös käyttäjätunnus ja salasana, joiden käytöstä hallintasovellus huolehtii. Hallinta-asema käy hakemassa palvelupyyntöjä halutuin väliajoin hallintatietokannasta. Näiden välinen liikenne on myös suojattu IPSecin avulla. Hallinta-asema sijaitsee sisäisissä palveluissa ja on siten suojattu palomuurilla myös sisäverkon käyttäjiltä. Hallinta-aseman ja reititti-mien välinen hallintaliikenne suojataan IPSecillä. IPSecin päällä voi kulkea esimerkiksi SNMP- tai telnet-liikennettä tarpeen mukaan.

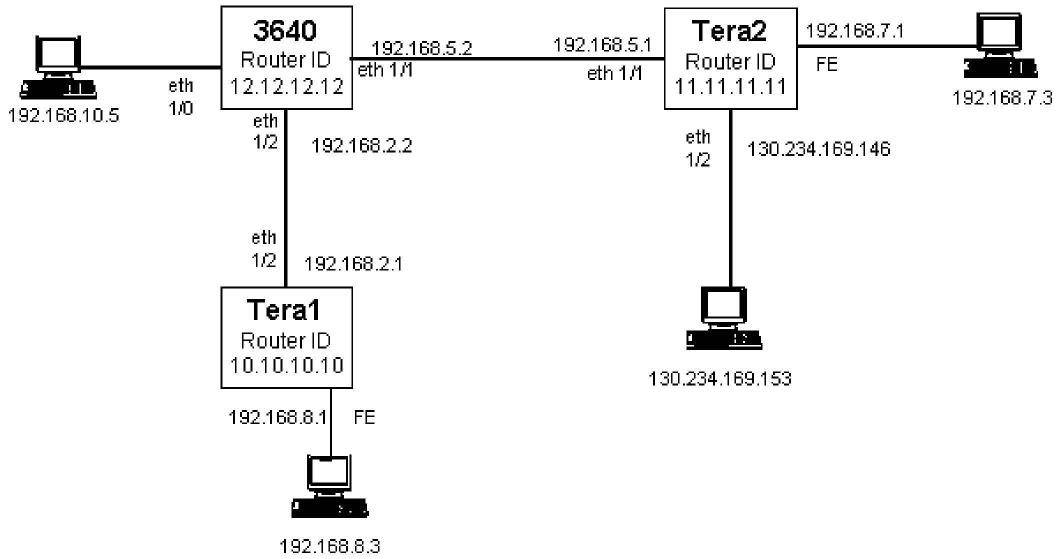


Kuva 6.28: Käytännön ratkaisu

6.3.3 Testiympäristö ja testit

Terabittiprojektissa testasimme hallinta-aseman ja reitittimien välisen yhteyden suojaamista IPSecillä. Testilaitteistoomme kuuluivat Linux RedHat 7.1 ja Windows 2000 -käyttöjärjestelmillä varustetut hallinta-asemat. Reitittiminä oli Cisco Systemsin 3640- ja 7000- sarjan malleja, joissa käyttöjärjestelmänä oli Ciscon oma *Internet*

Operating System (IOS) varustettuna *IPSec 3DES -lisäpaketilla*. Windowsissa käytimme sen omaa IPSec toteutusta. Linuxiin valitsimme ohjelmaksi FreeS/WANin [36] version 1.91, joka oli uusin versio testihetkellä syksyllä 2001. Testiverkko on kuvattu tarkemmin kuvassa 6.29 ja siinä hallittavina reitittiminä ovat Tera1 ja Tera2. Hallinta-asemia ovat 130.234.169.153 (Linux) ja 192.168.8.3 (Windows 2000). 3640 kuvaa tässä tapauksessa tavallista runkoreititintä, jossa ei ole IPSec-ominaisuuksia. Työasemalla 192.168.10.5 ei ole mitään tekemistä IPSecin kanssa, joten siihen voidaan testata yhteyksiä ilman IPSeciä. Työasema 192.168.7.3 on reitittimillä toteutetun IPSec VPN:n testaamista varten. Lisätietoja laitteiden ja ohjelmistojen asetuksista on kommentoituna liitteissä yksi ja kaksi. Windows-asetuksia on selitetty lähteessä [80].



Kuva 6.29: Terabitti-projektin IPSec-testiverkko

Testimme olivat yksinkertaisia toimivuustestejä, joissa havaitsimme yhteyksien onnistuvan eri laitteiden välillä ja salauksen toimivan. Testitapauksemme olivat seuraavat:

1. Linux -hallinta-asema $\longleftrightarrow$ reititin
2. Windows -hallinta-asema $\longleftrightarrow$ reititin
3. Reititin $\longleftrightarrow$ reititin
4. Yhteydet IPSec-laitteilta muihin kuin IPSec-laitteisiin

Testiemme pääkohteena oli Linuxin ja reitittimien välisen yhteyden kokeileminen. Laitoimme liitteissä näkyvät asetukset laitteisiimme ja sen jälkeen kokeilimme reitittimien hallintaa telnet-protokollalla. Ongelmia esiintyi RSA-avainten erilaisessa tallennustavassa reitittimien ja FreeS/WANin välillä. Sertifikaatteja käytettäessä tallennustapa on standardoitu, joten tämä ongelma poistuu. Emme kuitenkaan testanneet sertifikaattejen kanssa vaan käytimme etukäteen jaettua avainta (psk).

Testasimme myös Windows 2000 -käyttöjärjestelmästä yhteyttä reitittimelle. Windowsin kansainväliseen versioon täytyy olla asennettuna *vahvan salauksen lisäpaketti* (engl. *high encryption pack*), jotta siinä toimii 3DES. Ilman sitäkin voi 3DESin valita, mutta Windows käyttää vain DESiä, vaikka asetuksissa näkyisikin 3DES. Testasimme tämän yhteyden DESiä käyttämällä. Windowsin tarkat IPSec-asetukset on esitetty tutkielmasta erillisessä erikoistyössä [42], joka on tehty Terabitti-projektissa.

Reitittimien välillä testasimme IPSec VPN -yhteyksiä. Tämän testin tarkoitus oli kokeilla VPN:n toteuttamista ja reititysprotokollien suojaamista IPSecillä. IPSec sopii reititysprotokollien suojaamiseen hyvin, koska sen toiminta ei ole riippuvainen protokollista. Yhteydet toimivat normaalisti 192.168.8.3:n ja 192.168.7.3:n välillä ja liikenne oli salattua reitittimien välillä.

Neljännen testin ajatuksena oli testata IPSecin vaikutus muihin kuin IPSec-yhteyksiin. Tuloksena oli ettei IPSec vaikuttanut niihin mitenkään.

6.4 Ratkaisun arviointia

Yleinen ratkaisu vaikuttaa kaikin puolin hyvältä. Siinä yhdelläkään yhteysvälillä ei liiku salaamatonta ja todentamatonta liikennettä, mikä antaa hyvän suojan passiivisia hyökkäyksiä vastaan. Järjestelmän eri osien eristäminen palomuurien avulla lisää turvallisuutta ja hallittavuutta, joten käyttäjät saavat yhteyden vain hallintapalvelimelle eikä suoraan hallinta-asemalle tai reitittimiin. Hallintapalvelimen ja

-aseman yhteistoiminta hallintatietokannan kautta puolestaan antaa mahdollisuuden tarkastaa palvelupyyntöjen oikeellisuus vielä hallinta-asemalla, jos hyökkääjä on kuitenkin saanut luotetun yhteyden hallintapalvelimelle.

Käytännön ratkaisussa tietoliikenteen suojaamiseen on käytetty parhaita tällä hetkellä saatavilla olevia standardoituja protokollia ja se vaikuttaa siten hyvältä kokonaisuutena. TLS soveltuu hyvin WWW-yhteyden suojaamiseen, koska protokollaa on analysoitu melko paljon eikä siinä ole havaittu isompia ongelmia [66], [74]. Sitä käytetään myös monissa Internetissä toimivissa pankkipalveluissa.

Myös reitittimien ja hallinta-aseman suojaaminen IPSecillä tuntuu olevan kestävä ratkaisu. IPv6 on tulossa ja IPSec sisältyy siihen. Vaihtoehtoisesti tällä välillä voidaan käyttää tunnelointia jollakin tunnelointiprotokollalla kuten SSHv2 tai omaa fyysistä kaapelointia. Oman fyysisen kaapeloinnin tarve ei kuitenkaan poista salauksen tarvetta, koska kaapelia on mahdotonta vahtia jatkuvasti vahingoittamiselta tai kuuntelulta. Fyysisen kerroksen salausta ei ole standardoitu, joten sen käyttö voidaan myös unohtaa. Hallintaprotokollilla kuten SNMPv3 on omia tietoturvapalveluita, mutta niiden käyttö ei ole yhtä joustavaa kuin IPSecin [43]. IPSec on myös skaalautuvampi kuin SNMPv3:n tietoturvaominaisuuden, koska IPSecissä voi käyttää automaattista avaintenhallintaa ja julkisen avaimen järjestelmää. IPSec on myös parhaiten tuettu IPv6:n myötä tulevaisuudessa ja kuten liitteen neljä taulukosta näkyy myös, osa reititinvalmistajista tukee jo tällä hetkellä IPv6:tta ja IPSeciä.

7 Yhteenveto

Verkkojen kasvaminen, käyttäjien lisääntyminen ja tietoturvaongelmien tulo on luonut tarpeen verkon tietoturvan pohtimiselle. Asiakkaat vaativat laatua verkkoyhteyksiltään, mikä on lisännyt tarpeita verkonhallintajärjestelmille. Näiden kahden suuntauksen seurauksena myös verkonhallinnan tietoturva on noussut tärkeäksi kysymykseksi.

Verkon tietoturvan toteuttaminen organisaatiossa vaatii järjestelmällisyyttä ja suunnitelmallisuutta. Organisaation verkon tietoturvamalli on siten hyvä pohja turvallisten tietoliikennejärjestelmien suunnittelua varten. Yleisesti ottaen turvallinen verkko vaatii, että siihen kytketyt laitteet ovat turvallisia. Verkkohan on yhtä turvallinen kuin sen heikoin lenkki. Turvallisuutta verkkoon voi tuoda käyttäen erilaisia tietoturvapalveluita, joita ovat luottamuksellisuus, eheys, käytettävyys, todentaminen, kiistämättömyys ja pääsynvalvonta. Näitä palveluita toteutetaan usein kryptografisin menetelmin salaus- ja todennusalgoritmeilla ja niiden avulla torjutaan tietoturvaan kohdistuvia hyökkäyksiä. Käytännön toteutuksia organisaation verkossa ovat palomuurit ja hyökkäyksien havainnointijärjestelmät.

Verkoissa yleisimmin käytetyssä *Internet Protokollan versiossa 4* (IPv4) on tietoturvaongelmia. Näitä ongelmia korjaamaan on luotu *Internet Protocol Security* (IPSec), joka sisältyy *Internet Protokollan versioon 6* (IPv6). Lisäksi IPSec on standardoitu *Internet Engineering Task Forcen* (IETF) toimesta ja on siten hyvä vaihtoehto tietoturvapalveluiden tarjoamiseen verkoissa. IPSecin pääosat ovat *todennusotsikko*, *salausotsikko* ja *IKE-avaintenhallintaprotokolla*. Todennusotsikko takaa pakettien eheyden ja alkuperän. Salausotsikko huolehtii salauksesta sekä myös pakettien todennuksesta, mutta ei aivan yhtä kattavasti kuin todennusotsikko.

Verkonhallintajärjestelmät ovat kehittyneet keskittyneeseen suuntaan, jossa käyttöliittymä on irroitettu omaksi osakseen. Hallintajärjestelmää käytetään usein WWW-selaimen avulla ja verkon laitteiden konfigurointi tapahtuu hallintajärjestelmän palvelimelta. Näistä muodostuvat kaksi yhteysväliä, joiden tietoliikenne täytyy erityisesti suojata.

Käyttäjän WWW-selaimelta palveluntarjoajan hallintapalvelimelle yhteys suojataan *Transport Layer Security -protokollan* (TLS) avulla. Tähän ei ole muita kovin varteenotettavia vaihtoehtoja, koska TLS on niin laajasti käytössä tällä hetkellä.

Toinen suojattava väli verkonhallintayhteyksissä on yhteys hallinta-asemalta laitteille, jotka ovat usein reitittimiä. Tähän soveltuu hyvin IPSec. Se ei ota kantaa hallintaprotokollaan ja se on muodostumassa yleisimmäksi virtuaalisten erillisverkkojen (VPN) toteutustavaksi. Joissakin verkonhallinta- ja reititysprotokollissa on omat salaus- ja todennuspalvelunsa, mutta niiden ongelmana on käytettävän protokollan vaihdosta tuleva työ ja useampien protokollien samanaikainen käyttö. IPSecillä pystytään suojaamaan nämä kaikki ilman lisätyötä.

Tässä tutkielmassa jäi avoimeksi suunnitellun järjestelmän käytännön hyökkäyskestävyys ja skaalautuvuus suureen järjestelmään, koska käytännön testit ovat aikaa vieviä ja kokonaisen järjestelmän rakentaminen on kallista. Avoimeksi jäi myös julkisen avaimen järjestelmien, joita on käsitelty lähteessä [47], sopivuus verkonhallintajärjestelmän kanssa käytettäväksi.

IPSec-reitittimien lisääntyessä tässä tutkielmassa esityn mallin kaltaiset ratkaisut tulevat laajempaan käyttöön ja IPSec on koko ajan kehityksen alla [48], joten ratkaisun tulevaisuus vaikuttaa kestävältä. Myös aktiivisten ja oppivien järjestelmien, jotka tunnistavat uudenlaisia hyökkäyksiä vanhojen lisäksi, käyttö tulee lisääntymään. Asiakkaille tulee mahdollisuus valvoa oman yhteytensä laatua ja tulevaisuuden verkonhallintajärjestelmät saavat näin myös asiakkaiden luottamuksen.

Viitteet

[1] ”2002 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute, 2002

[2] ”A Comparison Between IPSec and Multiprotocol Label Switching Virtual Private Networks”, White Paper, Cisco Systems, 2000

[3] Allen J., Christie A. ja McHugh J., ”The Role of Intrusion Detection Systems”, IEEE Software, September/October 2000

[4] Allen C. ja Dierks T., ”The TLS Protocol Version 1.0”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2246.txt>, IETF, 1999

[5] ”Advanced Encryption Standard (AES)”, FIPS PUB 197, U.S. Department of Commerce, National Institute of Standards and Technology, WWW:ssä <URL:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, 2001

[6] Atkinson R. ja Kent S., ”IP Authentication Header”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2402.txt>, IETF, 1998

[7] Atkinson R. ja Kent S., ”IP Encapsulating Security Payload (ESP)”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2406.txt>, IETF, 1998

[8] Atkinson R. ja Kent S., ”Security Architecture for IP”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2401.txt>, IETF, 1998

[9] Alcatel, WWW:ssä <URL:http://www.alcatel.com>, viitattu 25.2.2002

[10] Allied Telesyn, WWW:ssä <URL:http://www.alliedtelesyn.co.nz>, viitattu 25.2.2002

[11] Aoki Kazumaro ja Lipmaa Helger, ”Fast Implementations of AES Candidates”, WWW:ssä <URL:http://www.tcs.hut.fi/~helger/papers/al00/fastaes.pdf>, 2000

[12] Adams R., Pereira R. ja Thayer R.,”The ESP CBC-Mode Cipher Algorithms”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2451.txt>, IETF, 1998

[13] Arkin Ofir, ”ICMP Usage In Scanning”, WWW:ssä <URL:http://www.sys-security.com/html/papers.html>, 2001

[14] Bauer Mick, ”Paranoid Penguin: Designing and Using DMZ Networks to Protect Internet Servers”, Linux Journal, Issue 83es, 2001

[15] Barker Elaine, Bassham Lawrence, Burr William, Dworkin Morris, Foti James, Nechvatal James ja Roback Edward, ”Report on the Development of the Advanced Encryption Standard (AES)”, U.S. Department of Commerce, National Institute of Standards and Technology, WWW:ssä <URL:http://csrc.nist.gov/encryption/aes/round2/r2report.pdf>, 2000

[16] Bellare M., Canetti R ja Krawczyk H., ”HMAC: Keyed-Hashing for Message Authentication”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2104.txt>, IETF, 1997

[17] Braun T., Günther M. ja Khalil I., ”An Architecture for Managing QoS-enabled VPNs over the Internet”, Proceedings of the 24th Conference on Local Computer Networks LCN’99, IEEE Computer Society, WWW:ssä <URL:http://www.iam.unibe.ch/řvs/publications/LCN99.pdf>, 1999

[18] Bourne T., Gaidosch T., Kunzinger C., Murhammer M., Rademacher L. ja Weinfurter A., ”A Guide to Virtual Private Networks”, Prentice-Hall, 1998

[19] Bellamy Jay, ”Market Survey: Virtual Private Networks”, WWW:ssä <URL:http://www.scmagazine.com/scmagazine/2001_09/survey/survey.html>, SC Magazine, September 2001

[20] Carrel D. ja Harkins D., ”The Internet Key Exchange (IKE)”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2409.txt>, IETF, 1998

[21] Cisco Systems, WWW:ssä <URL:http://www.cisco.com/>, viitattu 26.8.2002

[22] Common Criteria, WWW:ssä <URL:http://www.commoncriteria.org>, viitattu 28.10.2002

[23] Convery Sean ja Trudel Bernie, ”Cisco SAFE: A security blueprint for enterprise networks”, Cisco Systems, 2000

[24] ”Data Encryption Standard (DES)”, FIPS PUB 46-3, U.S. Department of Commerce, National Institute of Standards and Technology, 1999

[25] Deering S. ja Hinden R., ”Internet Protocol, Version 6 (IPv6) Specification”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2460.txt>, IETF, 1998

[26] ”DES Modes of Operation”, FIPS PUB 81, U.S. Department of Commerce, National Institute of Standards and Technology, WWW:ssä <URL:http://www.itl.nist.gov/fipspubs/fip81.htm>, 1980

[27] Doraswamy Naganand ja Harkins Dan, ”IPSec the New Security Standard for the Internet, Intranets, and Virtual Private Networks”, Prentice-Hall, First Edition, 1999

[28] Doraswamy N., Glenn R. ja Thayer R.,”IP Security Document Roadmap”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2411.txt>, IETF, 1998

[29] Deshaies Jane, ”FreeS/Wan Performance - Throughput doubled with AES”, WWW:ssä <URL:http://lists.freeswan.org/pipermail/users/2002-February/007771.html>, FreeS/WAN mailing list, viitattu 28.10.2002

[30] Extreme Networks, WWW:ssä <URL:http://www.extremenetworks.com>, viitattu 25.2.2002

[31] Frankel S., Glenn R. ja Kelly S., ”The AES Cipher Algorithm and Its Use With IPsec”, WWW:ssä <URL:http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt>, Internet Draft, IETF, 2002

[32] Frankel S. ja Herbert H., ”The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec”, WWW:ssä <URL:http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-xcbc-mac-02.txt>, Internet Draft, IETF, 2002

[33] Frankel S. ja Herbert H., ”The HMAC-SHA-256-128 Algorithm and Its Use With IPsec”, WWW:ssä <URL:http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-sha-256-01.txt>, Internet Draft, IETF, 2002

[34] Fraser B., ”Site Security Handbook”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2196.txt>, IETF, 1997

[35] Fites M., Kratz P. ja Brebner A., "Control and Security of Computer Information Systems", Computer Science Press, 1989

[36] FreeS/WAN, WWW:ssä <URL:http://www.freeswan.org/>, viitattu 28.10.2002

[37] Glenn R. ja Madson C., ”The Use of HMAC-MD5-96 within ESP and AH”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2403.txt>, IETF, 1998

[38] Glenn R. ja Madson C., ”The Use of HMAC-SHA-1-96 within ESP and AH”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2404.txt>, IETF, 1998

[39] GNU Privacy Guard (gpg), Release Notes, WWW:ssä <URL:http://www.gnupg.org/whatsnew.html>, viitattu 28.10.2002

[40] Govaerts René, Preneel Bart ja Vandewalle Joos, ”Hash Functions for Information Authentication”, ESAT Laboratorium, K.U. Leuven, 1992

[41] Hautaniemi Mika, ”TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta”, Teknillinen Korkeakoulu, WWW:ssä <URL:http://keskus.hut.fi/julkaisut/tyot/diplomityot/611/thesis.html>, 1994

[42] Heikkilä Tommi, ”Verkonhallintajärjestelmien tietoturva”, tietotekniikan erikoistyö, Jyväskylän yliopisto, Tietotekniikan laitos, 2001

[43] Hia H. E. ja Midkiff S., ”Securing SNMP across backbone networks”, Computer Communications and Networks, Proceedings, Tenth International Conference on , 2001

[44] Houle Kevin ja Weaver George, ”Trends in Denial of Service Attack Technology”, Carnegie Mellon University, CERT Coordination Center, WWW:ssä <URL:http://www.cert.org/archive/pdf/DoS_trends.pdf>, 2001

[45] Hämäläinen T., Vapa M., Wallenius E. ja Wikström M., ”Terabittiverkko – Nopea älyverkko”, Prosessori, Numero 13, 2000

[46] IANA, WWW:ssä <URL:http://www.iana.org/>, viitattu 28.10.2002

[47] Ilmarinen Sami ja Viinikainen Jukka, ”PKI-järjestelmien ja mobiililaitteiden yhteensovittaminen”, tietotekniikan pro gradu -tutkielma, Jyväskylän yliopisto, Tietotekniikan laitos, 2001

[48] IPSec working group, WWW:ssä <URL:http://www.ietf.org/html.charters/ipsec-charter.html>, IETF, viitattu 28.10.2002

[49] Juniper, WWW:ssä <URL:http://www.juniper.net>, viitattu 7.5.2002

[50] Kaario Kimmo, ”TCP/IP-verkot”, Docendo, 2002

[51] Kerttula Esa, ”Tietoverkkojen tietoturva”, Liikenneministeriö, Edita, 1998

[52] Keromytis A. ja Provos N., ”The Use of HMAC-RIPEMD-160-96 within ESP and AH”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2857.txt>, IETF, 2000

[53] Krawczyk Hugo, ”SKEME: A Versatile Secure Key Exchange Mechanism for Internet”, WWW:ssä <URL:http://www.research.ibm.com/security/skeme.ps>, IEEE, 1995

[54] Lamberg Juha, ”Palomuuri palveluna”, tietotekniikan pro gradu -tutkielma, Jyväskylän yliopisto, Tietotekniikan laitos, 2002

[55] Linux Intrusion Detection System, WWW:ssä <URL:http://www.lids.org/>, viitattu 6.9.2001

[56] Luoma Juha, ”Julkisten verkkojen käyttö verkkojen yhdistämisessä IPSEC-standardiin pohjautuvilla ratkaisuilla”, Diplomityö, Teknillinen korkeakoulu, Tietotekniikan osasto, 2000

[57] Marconi, WWW:ssä <URL:http://www.marconi.com>, viitattu 25.2.2002

[58] Messmer Ellen, ”Net routers still feeling effects of Code Red, Nimda”, WWW:ssä <URL:http://www.nwfusion.com/archive/2001/126341_10-15-2001.html>, Network World, 2001

[59] Menezes Alfred J., van Oorschot Paul C. ja Scott A. Vanstone, ”Handbook of Applied Cryptography”, WWW:ssä <URL:http://www.cacr.math.uwaterloo.ca/hac/>, Electronic version, 1996

[60] Maughan D., Schertler M., Schneider M. ja Turner J., ”Internet Security Association and Key Management Protocol (ISAKMP)”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2408.txt>, IETF, 1998

[61] ”Next-generation SSH Secure Shell offers support for PKI, Smart Cards and Advanced Encryption Standard”, lehdistötiedote, SSH Communications Security, WWW:ssä <URL:http://www.ssh.com/about/press/detail.cfm?id=285>, viitattu 21.3.2002

[62] Nikander Pekka, Peltonen Tapio ja Viljanen Lea, ”Internet tietoturva”, Suomen ATK-kustannus, 1996

[63] ”Open-Source Intrusion-Detection Tools for Linux ”, Linux Journal, Issue 78, 2000

[64] Oppliger Rolf, ”Security at the Internet Layer”, Computer, September (Vol. 31, No. 9), IEEE, 1998

[65] Orman H., ”The OAKLEY Key Determination Protocol”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2412.txt>, IETF, 1998

[66] Paulson Lawrence, ”Inductive Analysis of the Internet Protocol TLS”, ACM Transactions on Information and System Security, Vol. 2, No. 3, August 1999

[67] Piper D., ”The Internet IP Security Domain of Interpretation for ISAKMP”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc2407.txt>, IETF, 1998

[68] Park Kihong ja Lee Heejo, ”On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack”, INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE , Volume 1 , 2001

[69] Rivest R., ”The MD5 Message-Digest Algorithm”, WWW:ssä <URL:http://www.ietf.org/rfc/rfc1321.txt>, IETF, 1992

[70] Saarimäki Mikko, ”Diskreettiä ja äärellistä matematiikkaa, Matematiikan approbatur 3”, Jyväskylän yliopisto, Avoin yliopisto, 1997

[71] Schneier Bruce, ”Is 1024 Bits Enough?”, Crypto-Gram, Counterpane Internet Security, WWW:ssä <URL:http://www.counterpane.com/crypto-gram-0204.html>, Issue April 15, 2002

[72] Sano Fumihiko, Koike Masanobu, Kawamura Shinichi ja Shiba Masue, ”Performance Evaluation of AES Finalists on the High-End Smart Card”, U.S. Department of Commerce, National Institute of Standards and Technology, WWW:ssä <URL:http://csrc.nist.gov/encryption/aes/round2/conf3/papers/14-fsano.pdf>, viitattu 28.10.2002

[73] ”SSH Sentinel”, White Paper, SSH Communications Security, WWW:ssä <http://www.ssh.com/tech/whitepapers/SSH_Sentinel_White_Paper.pdf>, 2001

[74] Schneier B. ja Wagner D., ”Analysis of the SSL 3.0 protocol”, WWW:ssä <http://www.counterpane.com/ssl.html>, The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, 1996

[75] ”Secure Hash Standard”, FIPS PUB 180-1, U.S. Department of Commerce, National Institute of Standards and Technology, 1995

[76] Snort, WWW:ssä <URL:http://www.snort.org/>, viitattu 28.10.2002

[77] Staats Robert, ”Making a Case for MPLS VPNs over Traditional VPNs”, Cisco World, April 2001

[78] Stallings William, ”Cryptography and Network Security: Principles and Practice”, Second Edition, Prentice-Hall, 1999

[79] Stallings William, ”SNMP, SNMPv2, SNMPv3, and RMON 1 and 2”, Addison Wesley Longman, 1999

[80] Takkinen Sauli, ”IPSecin käyttö Active Directory -pohjaisessa mikrotietokoneverkossa”, tietotekniikan pro gradu -tutkielma, Jyväskylän yliopisto, Tietotekniikan laitos, 2002

[81] ”Telecommunications management network”, ITU-T Recommendation M.3010, 05/96

[82] Vaarala Sami, ”Implementing Internet Key Exchange (IKE)”, Master's Thesis, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2000

[83] ”Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta”, Valtiovarainministeriö, 1999

[84] ”Valtionhallinnon tietoturvallisuuskäsitteistö”, WWW:ssä <URL:http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/sanasto/sisallys.htm>, Valtiovarainministeriö, 2000

[85] Vapa Mikko, ”A Solution for Managing Quality of Service in Internet Protocol Networks”, tietoliikenteen pro gradu -tutkielma, Jyväskylän yliopisto, Tietotekniikan laitos, 2000

[86] WBEM-standardi, WWW:ssä <URL:http://www.dmtf.org/standards/standard_wbem.php>, viitattu 28.10.2002

[87] ”Yritysturvallisuus”, WWW:ssä <URL:http://www.ytnk.fi/baletti.html>, Yritysturvallisuus TT-PT, viitattu 28.10.2002

Liite 1. Linuxin IPSec-asetukset

FreeS/WAN

Linuxissa käytimme IPSec-ohjelmistona FreeS/WANin versiota 1.91. Asennukseen löytyy hyvät ohjeet projektin kotisivulta, joten tässä ei kerrota sen enempää asennuksesta. Uusin versio löytyy myös edellä mainitulta kotisivulta, Myöhemmissä versioissa on tuki uusimmille 2.4 sarjan kerneleille. Ainakin kernel versioon 2.4.6 saakka 1.91 toimii ilman muutoksia. FreeS/WANin asetustiedosto *ipsec.conf* on hyvin tarkka muodostaan ja sinne ei saa lisätä väliin tyhjiä rivejä. FreeS/WAN ilmoittaa rivinumeron, jolla virhe on ja muotoseikat on helppo korjata niiden ilmetessä. Kannattaa noudattaa ohjelman mukana tulevan esimerkkitiedoston mallia. Tässä dokumentissa muoto ei ole välttämättä oikea, koska sitä on jälkikäteen kommentoitu. Kommenttimerkki tiedostossa on #. Etukäteen jaettu avain (psk) kirjoitetaan tiedostoon ipsec.secrets. Samasta tiedostosta löytyy myös RSA-avaimet. Lisäselityksiä tiedoston kohdista löytyy ohjelman dokumentaatiosta. FreeS/WAN ei tue DESiä, mutta se on saatavilla ainakin versioon 1.9 erillisenä osana. Se on testattu toimivaksi Ciscon IOS:n kanssa. [36]

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
# More elaborate and more varied sample configurations can be found
# in FreeS/WAN's doc/examples file, and in the HTML documentation.
# basic configuration eli yleiset asetukset
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute on OK yleensä. Voi laittaa suoraan
        # verkkokortin, esim. eth0
        interfaces=%defaultroute
        forwardcontrol=no
        # Debug-logging controls:  "none" for (almost) none,
        # "all" for lots.
        klipsdebug=none
        plutodebug=none
        # Use auto= parameters in conn descriptions
```

```
        # to control startup actions.
        plutoload=%search
        plutostart=%search
        plutowait=no
        # Close down old connection when new one
        # using same ID shows up.
        # Eli ei voi avata kahta samaa yhteyttä
        uniqueids=yes

# Yhteyskohtaiset asetukset Linuxin ja
# Ciscon 7200 -reitittimen yhdistämiseen
conn terap-7200
# authby, secret=PSK, jos RSA-avainta niin  authby=rsasig
# (emme saaneet toimimaan sitä Ciscon kanssa)
        authby=secret
#  Tunnelimoodia suositellaan käytettäväksi
        type=tunnel
# How persistent to be in (re)keying negotiations (0 means very).
# for testing only keyingtries=1, for production keyingtries=0
        keyingtries=1
# Hallinta-aseman osoite = left
        left=130.234.169.153
# Reitittimen osoite = right
        right=130.234.169.145
# Seuraava osoite, johon paketit menee
        leftnexthop=130.234.169.129
        rightnexthop=130.234.169.129
# Käytetään IKEä eli automaattinen avaintenvaihto
        keyexchange=ike
# Avaimen ikä 3600 sekuntia
        keylife=3600s
# Perfect Forward Secrecy = yes
        pfs=yes
# Ladataan parametrit muistiin käynnistettäessä
```

```
        auto=add
# Ehdotus salausalgoritmiksi ja tiivistefunktioksi
        esp=3des-sha1-96
```

Liite 2. Reitittimien IPSec-asetukset

Ciscon IPSec-asetukset

Ciscon IOS täytyy olla varustettu IPSec DES tai 3DES feature packilla, jotta IPSeciä voisi käyttää. 3DES-versio täytyy olla käytössä, jos reititintä käytetään FS/WANin kanssa, koska FS/WAN ei tue DES:a.

Vianetsintäasetukset

Vianetsintään ja IPSecin toiminnan tarkkailuun sopii seuraavat komennot.

```
# debug crypto engine                     Crypto Engine Debug
# debug crypto ipsec                      IPSEC processing
# debug crypto isakmp                     ISAKMP Key Management
# debug crypto key-exchange               Key Exchanger
# debug crypto pki                        PKI Client
# debug crypto sessmgmt                   Session Management
# show crypto engine connections active   Active crypto connections
```

Muut asetukset

Tässä on asetukset toiselle reitittimelle (IPSec VPN) ja Windowsille (hallintayhteys). Tera2:n kohdalla tulee FreeS/WAN-yhteyden asetukset. Reitittimien väliseen todennukseen voidaan käyttää RSA-avaimia. Windowsin kanssa emme käyttäneet PFS:ä (se puuttuu seuraavasta listauksesta).

Tera1

```
crypto isakmp policy 1       ! ISAKMP politiikka 1
 authentication pre-share    ! Käytetään psk:tä,
 group 2                     ! Diffie-Hellman ryhmä 2
 lifetime 3600               ! Ikä 3600 sekuntia
!
crypto isakmp policy 2
 authentication pre-share    ! Tässä voisi olla myös RSA
 group 2
 lifetime 3600
!
crypto isakmp key tera address 192.168.5.1 ! psk tera Tera2:sta varten
crypto isakmp key win address 192.168.8.3  ! psk win Windowsia varten
!
! Windowsin kanssa käytettävä salausalgoritmi ja tiivistefunktio
! (muista käyttää samaa Windowsissa).
crypto ipsec transform-set win esp-des esp-sha-hmac
! Toisen reitittimen kanssa käytettävä salausalgoritmi
! ja tiivistefunktio.
crypto ipsec transform-set tera esp-3des esp-sha-hmac
!
! RSA-avain allekirjoitusta varten, jos käytetään RSA:ta
! osapuolen tunnistamiseen.
! Tämä toimi reitittimien välillä. Windowsin kanssa käytetään psk:tä.
crypto key pubkey-chain rsa
 addressed-key 192.168.5.1 signature
  address 192.168.5.1
  key-string        ! Public Key
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00E45F5B 6FC68C7A 8EF5D748 0D825477 0812840A 04C14028 5B5FC378 51E9C1EA
   05BB08EA 35FFD392 230828C6 B29EF6EB 1DA464CE 1265581E EB629D49 E38D44EE
   FAFEFBEA 89270CA5 0C09756E 46440ECD 0FE27F02 64862A82 DCF3B84B 3F2C715D
   FFDD809A 61AAD2F4 D4A377C8 082E1872 DCC8C824 7F691B87 62614174 B2F7E2CC
```

```
    338741F8 4A690F5C 8F22F663 3F127835 2E850FE0 CD1C502B DE793652 DF5A313C
    C4CE3893 8FFDD98F 7EB91BC9 27C6E839 215A3A5D 81D480A9 7CE510E4 BA64AF85
    9A9F6288 624582C4 E3A71B4D 83495145 C4DB8EC0 C7F9C43D C22FD4A0 27DD5728
    41157DA7 6F2549B0 9301F279 1CB3EBA3 E716C817 0B1DB981 5EF6E8F7 0E024497
    99020301 0001
   quit
  !
! Crypto map Windows 2000 -yhteyttä varten.
 crypto map win 1 ipsec-isakmp
 set peer 192.168.8.3       ! Windowsin IP-osoite
 set transform-set win      ! Aikaisemmin määritelty transform set käyttöön
 match address 199      ! Access listin numero
! Crypto map toista reititintä varten (IPSec VPN)
crypto map tera 2 ipsec-isakmp
 set peer 192.168.5.1       ! TERA2:n IP-osoite
 set transform-set tera     ! Aikaisemmin määritelty transform set käyttöön
 match address 190      ! Access listin numero
!
interface Ethernet1/2       ! Liitäntä, jossa halutaan käyttää IPSeciä
 ip address 192.168.2.1 255.255.255.224
 no ip redirects
 no ip directed-broadcast
 no cdp enable
crypto map tera     ! Kytketään crypto map tera vain tähän liitäntään
! Kytketään crypto map win samoin omaan liitäntään
! Access-list -asetukset
! IPSec VPN -asetukset, VPN 192.168.7.* ja 192.168.8.* -verkon välille
access-list 190 permit ip 192.168.7.0 0.0.0.255 192.168.8.0 0.0.0.255
access-list 190 permit ip 192.168.8.0 0.0.0.255 192.168.7.0 0.0.0.255
! Annetaan oikeus Windows hallinta-aseman ja reitittimen
! väliselle liikenteelle
access-list 199 permit ip host 192.168.8.3 host 192.168.8.1
access-list 199 permit ip host 192.168.8.1 host 192.168.8.3
```

Tera2

```
ip domain-name jyu.fi
!
crypto isakmp policy 1
 authentication pre-share
 group 2
 lifetime 3600
!
crypto isakmp policy 2
 authentication pre-share
 group 2
 lifetime 3600
! Jaettu avain tera reitittimien väliseen todentamiseen
crypto isakmp key tera address 192.168.2.1
! Jaettu avain 12345678 Linuxin ja reitittimen väliseen todentamiseen
crypto isakmp key 12345678 address 130.234.169.153
!
! Salausalgoritmien ja tiivistefunktioiden määritys yhteyksille
crypto ipsec transform-set linux esp-3des esp-sha-hmac
crypto ipsec transform-set tera esp-3des esp-sha-hmac
!
! RSA-avain allekirjoitusta varten, jos käytetään RSA:ta osapuolen
! tunnistamiseen. Tämä toimii reitittimien välillä.
! Linuxin kanssa käytetään psk:tä, koska emme saaneet sitä
! toimimaan FreeS/WANin kanssa.
crypto key pubkey-chain rsa
 addressed-key 192.168.2.1 signature
  address 192.168.2.1
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00A5AD83 C68280E2 BA4FAF4B C7117585 B46CF400 10966EBD BF37C5C6 25639BE8
   8803BBF1 D0AF4E98 6975C0C6 C0269541 E4074C53 285AF671 58ACA706 7D16AC96
   AAC66C6F B05F8FB8 5E98E530 792FFD73 4574A5E2 DC639565 F2960FD9 D46E8963
```

```
   85097A86 5FFCDFD2 2C17F319 761A385F 0AD88F97 643EDA6B 63E8BE61 1BD11567
   091E43CD AA4BC9A5 B8FD600F 9560D62C 7C292A51 4087E4A3 9FA03240 5DCF9D0F
   3DFE7976 7D79B552 0AB499ED C047DB85 5CE21913 F904D3CD 0276CAB5 0ADB0A30
   05868DEC C88A2D85 84320760 A7F9BAA6 186366C6 8E5329A2 8B06DCAC 31A9B3EE
   B85C6C48 C84957 B3277C57 5B2B4D77 F0D12373 816826EA 30A062C7 44D24372
   E9020301 0001
  quit
 !
 ! Käytetään ISAKMP politiikka 1 linuxin kanssa
 crypto map linux 1 ipsec-isakmp
 set peer 130.234.169.153       ! Linuxin osoite
 set transform-set linux
 match address 199              ! Kytkettävä Access-list
crypto map tera 2 ipsec-isakmp  ! Reitittimien välillä 2:sta
 set peer 192.168.2.1           ! Toinen reititin
 set transform-set tera
 match address 190
! Crypto mappien käyttöönotto kytkemällä ne liitäntöihin
interface Ethernet1/1
 ip address 192.168.5.1 255.255.255.224
 no ip redirects
 no ip directed-broadcast
 no ip mroute-cache
 no cdp enable
 crypto map tera
!
interface Ethernet1/2
 ip address 130.234.169.146 255.255.255.224
 no ip redirects
 no ip directed-broadcast
 no ip mroute-cache
 no cdp enable
 crypto map linux
!
```

```
! Access-list -asetukset
! IPSec VPN -asetukset, VPN 192.168.7.* ja 192.168.8.* -verkon välille
access-list 190 permit ip 192.168.7.0 0.0.0.255 192.168.8.0 0.0.0.255
access-list 190 permit ip 192.168.8.0 0.0.0.255 192.168.7.0 0.0.0.255
! Annetaan oikeus Linux hallinta-aseman ja reitittimen
! väliselle liikenteelle
access-list 199 permit ip host 130.234.169.153 host 130.234.169.146
access-list 199 permit ip host 130.234.169.146 host 130.234.169.153
```

Liite 3. Reitittimien IPSec- ja SSH-tuki

Tutkin kuuden reititinvalmistajan kotisivulta heidän laitteidensa tukea IPSec:lle, SSH:lle ja IPv6:lle. Tulokset ovat alla taulukoituna. Joillakin sivuilla oli asetettu tietoa hyvin epämääräisesti eikä niistä käynyt kunnolla selville tuki, joten taulukkoon on suhtauduttava erittäin suurella varauksella. Laitteiden tuki paranee koko ajan, joten kannattaa tarkistaa tämän hetken tilanne ei-vastausten kohdalta valmistajien sivuilta. Täytyy huomioida vielä, että IPSecin pitäisi sisältyä IPv6-toteutuksiin. IPSec tarkoittaakin IPSec-tukea IPv4:lle. Ciscon IPSec-tuen olemme testanneet lisäksi käytännössä.

Valmistaja	SSH	IPSec	IPv6
Alcatel	ei	ainakin VPN-tuotteissa	ei
Allied Telesyn	versio 1.5	kyllä	ei
Cisco Systems	versio 1	kyllä	kyllä
Extreme Networks	versio 2	ei	ei
Juniper	versio 2	kyllä	osassa tuotteita
Marconi	ei	kyllä	kyllä

Taulukko 7.8: Protokollatuki eri valmistajien laitteissa [57], [9], [30], [10], [49], [21]

Hakemisto