Niko Arnivaara

MB Connect Line tietoturvallinen etäyhteysjärjestelmä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Kone- ja tuotantotekniikka

Insinöörityö

25.10.2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Niko Arnivaara MB Connect Line tietoturvallinen etäyhteysjärjestelmä 42 sivua + 2 liitettä 25.10.2018
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Kone- ja tuotantotekniikka
Ohjaajat	Myyntipäällikkö Sami Suokas Lehtori Pekka Salonen

Insinöörityön tarkoituksena oli tutkia MB Connect Linen tarjoaman M2M-tiedonkeruu- ja etäyhteysjärjestelmän teknisiä ominaisuuksia, tieto- ja kyberturvallisuutta sekä IOT:n ja M2M-yhteyden eroavaisuuksia. Tietoliikennetekniikassa on 5G-sukupolven teknologian myötä tapahtumassa paljon uusia kehitysinnovaatioita. 5G tulee toteutuessaan mullistamaan tiedonsiirtonopeudet verrattuna nykyiseen 4G-sukupolven LTE-teknologiaan.

Langaton tiedonsiirtoteknologia ei kuitenkaan ole aivan ongelmatonta. Eri vaihtoehdoista löytyy niin hyviä kuin huonojakin puolia.

Työssä tutustuttiin kyber- ja tietoturvasuojaa antaviin salausprotokolliin, joita etäyhteyksissä on käytössä. Yleisimmin käytettyjä salaustekniikoita ovat VPN- ja SSL/TLS-tekniikat, joihin työssä lähinnä keskityttiin.

Lisäksi tehtiin ohjeistus palveluna tarjottavasta reitittimen konfiguroinnista.

Avainsanat	Teollisuuden etäyhteysjärjestelmä, Internet of Things, Machine to Machine, VPN-yhteys

Author	Niko Arnivaara
Title	Data Security Remote System of MB Connect line
Number of Pages	42 pages + 2 appendices
Date	25 October 2018
Degree	Bachelor of Engineering
Degree Programme	Mechanical and Production Engineering
Instructors	Sami Suokas, Sales Manager Pekka Salonen, Senior Lecturer

The objective of the Bachelor's thesis was to investigate the M2M data collection and the features of the remote technology system.

In addition, the aim was to examine cybersecurity, and IOT and M2M connectivity provided by MB Connect Line. In telecommunication technology, several new development innovations are taking place with 5G generation technology. 5G networks will, when implemented revolutionize data transfer speeds compared to the 4G -generation LTE-technology.

However, wireless data transfer technology is not quite problematic. There currently exist various alternatives that offer benefits but they may also bring disadvantages.

In the thesis, cyber and data security encryption protocols are analyzed, which are used in remote connections. The most commonly used cryptographic techniques are VPN and SSL / TLS, which the author mainly focused on in the thesis.

In addition, instructions for router configuration were carried out. The router configuration is offered to customers as a service.

Keywords	Industrial remote system, Internet of Things, Machine to Machine, VPN-connection

Sisällys

Lyhenteet

3DES	*Triple Data Encryption Standard.* DES-salausmuodon kehittyneempi versio.
AES	*Advanced Encryption Standard.* Lohkosalausmenetelmä, jota käytetään tietotekniikassa. AES on Yhdysvaltain standardoimisviraston standardoima seuraaja DES:lle.
AH	*Authentic Headers*. AH tarjoaa todennuksen ja takaa viestien eheyden.
COMSEC	*Communication Security*. Tietoturvallisuuden toiminnoilla tarkoitetaan tietoturvallisuuden testausta, hyväksyntää ja valvontaa.
DES	*Data Encryption Standard.* On Yhdysvalloissa liittovaltion standardiksi 1976 valittu salausmenetelmä, jota on käytetty laajasti ympäri maailmaa.
DSA	*Digital Signature Algorithm.* Digitaalinen allekirjoitusalgoritmi sähköisille allekirjoituksille.
ESP	*Encapsulating Security Payloads*. ESP:tä käytetään pakettivirtojen salaamiseen.
FTP	*File Transfer Protocol*. Internetin TCP/IP-protokolla, joka määrittelee tiedostojen siirron palvelimesta toiseen tietoverkon välityksellä.
GPRS	*General Packet Radio System*. GSM-verkossa toimiva pakettikytkentäinen tiedonsiirtopalvelu, jota käytetään pääasiassa langattoman internet-yhteyden muodostamiseen mobiilitietokoneissa.
GSM	*Global System for Mobile communications*. Matkapuhelinjärjestelmä, jota käytetään maailmanlaajuisesti.
HTTP	*Hyper Text Transfer Protocol*. Internetin TCP/IP-protokolla, joka määrittelee WWW-dokumenttien siirron tietoverkon yli.

HTTPS	*Hyper Text Transfer Protocol Secure*. HTTP-protokollan ja TLS / SSL-protokollan yhdistelmä, jota käytetään tiedon suojattuun siirtoon WEB:ssä.
IDEA	*International Data Encryption Algorithm.* Kryptografisesti vahva 64-bittinen lohkosalaaja, jonka avaimen pituus on 128-bittiä.
IIOT	*Industrial Internet of Things*. Teollinen internet.
IKE	*Internet Key Exchange*. IPSec-protokollan kanssa käytettäväksi suositeltu avaintenvaihtoprotokolla.
IOT	*Internet Of Things*. Esineiden internet.
IPSEC	*IP Security Architecture*. Joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia internet-yhteyden turvaamiseksi.
L2TP	*Layer to Tunneling Protocol*. Microsoftin ja Ciscon kehittämä VPN-tunnelointiprotokolla, joka toimii OSI-mallin 2. kerroksella.
LTE	*Long-Term Evolution*. Edistynyt 3G-tekniikka, jonka tarkoitus on kasvattaa datan tiedonsiirtonopeuksia, lyhentää viiveitä, parantaa palveluita ja vähentää kuluja. Myös kutsuttu 4G:ksi.
M2M	*Machine to Machine*. Koneiden välinen älykäs kommunikointi.
MPI	*Multi-Point Interface.* Siemensin ohjelmoitavan logiikkaohjaimen SIMATIC S7 oma käyttöliittymä.
OSI-malli	*Open System Interconnection Reference Model*. Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PPTP	*Point to Point Tunneling Protocol*. VPN-tunnelointiprotokolla, joka pohjautuu PPP-protokollaan.
RSA	*Rivest, Shamir, Adleman.* Julkisen avaimen salausalgoritmi.

SMTP *Simple Mail Transfer Protocol*. Internetin alkuperäinen sähköpostiprotokolla. SMTP tukee vain seitsemänbittisiä merkkejä, joten kahdeksanbittisten merkkien (Å, Ä ja Ö) esittämiseksi on jouduttu kehittämään monia kiertoteitä.

SPI *Security Parameter Index.* Suojausparametrin indeksi on tunnistekoodi, joka lisätään otsikkoon, kun käytetään IPSec-protokollaa IP-liikenteen tunnelointiin. Tämä tunniste auttaa ydintä erottelemaan kahden eri liikennevirran välillä, joissa voi olla käytössä eri salaussääntöjä ja algoritmeja.

SSL *Secure Socket Layer*. Yleisin käytössä oleva salausprotokolla internetin käytössä.

TLS *Transport Layer Security*. Aiemmin tunnettu lyhenteen SSL, salausprotokolla, jolla voidaan suojata internet-sovellusten tietoliikenne IP-verkkojen yli.

UMTS *Universal Mobile Telecommunications System*. GSM:n seuraajaksi suunniteltu kolmannen sukupolven matkapuhelinteknologia.

VPLS *Virtual Private LAN Service*. Virtuaalinen yksityinen LAN-palvelu on tapa tarjota Ethernet-pohjainen monipisteestä monipisteeseen-yhteys IP- tai MPLS-verkon yli.

VPN *Virtual Private Network*. Virtuaalinen erillisverkko on tapa, jolla kaksi tai useampia verkkoja voidaan yhdistää julkisen verkon yli siten, että ne muodostavat näennäisesti yksityisen verkon.

WEB *World Wide Web tai WWW*. Internet-verkossa toimiva hajautettu hypertekstijärjestelmä.

1 Johdanto

Tarkoituksena oli tutkia erityyppisiä etäyhteyden mahdollistavia verkkotekniikoita sekä tietoturvallisia tiedonsiirtoprotokollia. Aihe on erittäin ajankohtainen useille koneenvalmistajille ympäri Suomea, koska IOT (Internet of Things) on jälleen noussut erittäin suureksi puheenaiheeksi ja useat yritykset miettivät, miten hyödyntää IOT-tekniikkaa liiketoiminnassaan. Langattomassa verkkotekniikassa olemme seuraavaksi siirtymässä jo 5G-tekniikkaan. Tämä on hyvin kilpailtu alue kolmen suurimman (Nokia, Ericsson, Huawei) verkkovalmistajan keskuudessa, ja siksi siitä ei ole vielä materiaalia saatavilla, joten tässä työssä pitäydytään vielä 3G- ja 4G-verkkotekniikoissa. Etäyhteysreitittimenä tarkastellaan MB Connect Linen tuotteita, jotka ovat Suomessa Sarlin Oy Ab:n edustuksessa.

Sarlin Oy Ab on osa Sarlin Group Oy:tä oleva kotimainen perheyhtiö, joka tarjoaa teknisiä tuotteita, ratkaisuja ja palveluja teollisuudelle ja kunnille. Toiminnan lähtökohtana on asiantuntemus ja palvelut sekä asiakkaan odotuksiin vastaaminen. Sarlin Oy Ab:n organisaatio koostuu kolmesta eri yksiköstä, joita ovat automaatio, energia ja paineilma. Henkilöstön määrä Sarlin Group Oy:ssä on 268 työntekijää, ja liiketoimintayksiköitä ovat Sarlin Oy Ab, Sarlin Furnaces Ab sekä Beamex Oy Ab.

MB Connect Line GmbH on perustettu Saksassa vuonna 1997 Werner Bellen ja Siegfried Müllerin toimesta, ja heidän arvoihinsa on alusta asti kuulunut ”Made in Germany”. Pääkonttorista hoidetaan myynti-, vienti- ja hallinnolliset toimenpiteet, ja se sijaitsee Ilsfeldissä. Tuotekehitys sijaitsee Dinkelsbühlissa. Yrityksen tuotteisiin kuuluvat pääasiassa mbNET-teollisuusreitittimet, jotka ovat kehittyneet jo toiseen sukupolveen. Laitteet on varustettu integroiduin 4-porttisin kytkimin. Siemens S7-järjestelmä voidaan yhdistää suoraan MPI/profibusliitäntään. Lisäksi yli 90 ajuria on saatavilla sarjaliitäntään eri valmistajien kontrollointijärjestelmiin, operointipaneeleihin, taajuusmuuttajiin sekä inverttereihin. Uusi etäpalvelualusta mbCONNECT24 tarjoaa koneenrakentajalle tai koneenvalvojalle laaja-alaisen ratkaisun etäkunnossapitoon ja tiedonkeräämiseen sekä M2M (Machine to Machine)-yhteydet. Kaikki tarvittavat palvelut ja funktiot on integroitu keskitettyyn WEB-pohjaiseen alustaan. Se sopii niin tuotantolinjoihin ja kunnossapitoinfrastruktuuriin kuin myös laitossektorille ja mobileihin työkoneisiin. Käytännössä ei ole merkitystä, onko kyseessä pakkauskone, tuotantolinja, aurinkoenergia-

voimala tai biokaasulaitos. MB Connect Linella on tarjota toimiva etäyhteysjärjestelmä, joka muuttaa huolto-osaston tulosyksiköksi erittäin tietoturvallisesti.

2 Etäyhteysjärjestelmät ja niiden edut

Langattomia verkkoja hyväksi käyttäen etäyhteysjärjestelmillä on paljon käyttömahdollisuuksia, kun prosessia on mahdollista seurata käytännössä mistäpäin maailmaa tahansa, missä vain on toimiva internet yhteys. Suomi on yksi johtavia maita materiaalinkäsittelykoneiden valmistuksessa. Yleensä kone voi valmistuksen jälkeen sijaita ihan missä päin maailmaa tahansa, joten ainakin koneen vikaantumistilanteessa on ehdottoman tärkeää saada yhteys koneen vikatietokantaan ja siten selvyys, mitä todellisuudessa on tapahtunut. Toinen käytännön esimerkki voi olla esimerkiksi aurinkovoimaloiden valvonta. Pääasiassa aurinkovoimala kannattaa rakentaa mahdollisimman lähelle päiväntasaajaa, jossa on eniten aurinkoisia päiviä vuodessa. Langaton etäyhteys mahdollistaa kaikkien henkilöiden pääsyn reaaliaikaisiin tietokantoihin riippumatta siitä, onko henkilö paikan päällä vai ei. Tällaisilla ominaisuuksilla säästyy aikaa, vaivaa ja kustannuksia niin yrityksien kuin henkilöstönkin osalta.

2.1 Esineiden internet

IOT:lle löytyy kirjallisuudesta useita eri määritelmiä, jotka ovat osittain päällekkäisiä, mutta ne ovat kuitenkin eroteltavissa ja ovat kaikki osaltaan oikeita. Kun keskitytään pääasiassa identiteettiin, toiminnallisuuteen ja virtuaalisuuteen, niin voidaan IOT määritellä tuotteiksi, joilla on identiteetti virtuaalisessa ympäristössä ja jotka toimivat käyttäen älykästä rajapintaa kytkeytymiseen ja kommunikointiin älykkäissä ympäristöissä ja käyttäjäyhteyksissä. Sen voidaan katsoa olevan standardoituihin kommunikointiprotokolliin perustuva maailmanlaajuinen verkko, jossa jokainen tuote on osoitteellaan yksilöity ja liitetty yhteen [1].

Kun älykkäitä laitteita liitetään internetiin, niin ollaan huolissaan sekä nykyisen että tulevan internetin infrastruktuurista, Web-standardien soveltuvuudesta ja IP-(Internet Protocol) protokollapinosta. Koska internetiin suuntautunut näkemys painottaa koko verkon infrastruktuuria, niin tästä näkökulmasta huomioiden IOT määritellään seuraavasti:

> ”Globaali verkkoinfrastruktuuri, jonka tarkoituksena on yhdistää fyysiset ja virtuaaliset yhteydet informaationkeruuta ja kommunikointivalmiuksia hyväksikäyttäen. Rakenne sisältää jo olemassa olevaa sekä edelleen kehittyvää internetiä ja globaalin verkon kehityksiä. Se tarjoaa erityistä kohteentunnistusta ja anturi- että liitäntävalmiuksia perustana palvelujen ja sovellusten kehittämiselle. Nämä palvelut ja sovellukset ovat tunnettuja korkean asteen itsenäisestä tiedonkeruusta, tiedonsiirrosta, verkon liitettävyydestä ja yhteen toimivuudesta.” [1, s.10].

Yleisesti keskitytään systemaattiseen lähestymiseen tiedon mittaamisessa, visualisoinnissa, organisoimisessa ja tallentamisessa. Kun IOT:a lähestytään semanttista teknologiaa käyttäen:

> “Semanttisten teknologioiden sovellus edistää yhteen toimivuutta IOT:n resurssien, tietomallien, datatarjoajien ja kuluttajien välillä. Se helpottaa tehokasta tietojen saatavuutta ja integraatiota, resurssien löytämistä, semanttista päättelyä ja tietämyksen koostamista tehokkaiden menetelmien kautta, jotka voivat jäsentää, kommentoida, jakaa ja tehdä ymmärrettäväksi IOT:n datan ja helpottaa sen muuttamista toiminnalliseksi tietämykseksi ja älykkyydeksi erilaisilla sovellusaloilla.” [1, s. 10].

2.2 Teollinen internet

IIoT (Industrial Internet of Things) eli teollinen internet tarkoittaa koneita ja laitteita, jotka kommunikoivat keskenään, keräävät dataa ja käyttävät internetiä tiedonsiirtämiseen. Ympäristöä ja koneentoimintaa mitataan antureilla ja tieto lähetetään eteenpäin ohjelmistojen ja tietoliikenneyhteyksien avulla. Kerätyn datan avulla koneet voivat optimoida toimintaansa automaattisesti tai niitä voidaan hallita etäyhteyden avulla. Tietoa analysoimalla voidaan tehdä trendejä ja ennakoida huollon tarvetta. Yritykset pystyvät IIoT-ratkaisuja hyväksi käyttäen parantamaan tuottavuutta ja laitteiden kilpailukykyä. Koneiden välinen kommunikointi mahdollistaa myös kaukana sijaitsevien asiakkaiden palvelemisen.

2.3 Esineiden internet vs. koneiden välinen kommunikointi

Viime vuosina on ollut paljon puhetta IOT:sta ja sen eduista tilaajalle ja palveluntarjoajille, mutta tietoliikennepalvelujen tarjoajille on aiheutunut sekaannusta siitä, mitä eroa IOT:lla ja M2M-yhteyksillä todellisuudessa on. Tämä sekaannus johtuu väärinkäsityksistä, kun verrataan kahta samankaltaista asiaa toisiinsa. Eroavaisuuksia on lueteltu taulukossa 1.

Taulukko 1. M2M:n ja IOT:n eroavaisuudet [2].

M2M	IOT
P2P (point-to-point)-yhteys, tyypillisesti integroitu laitteistoon asiakkaan päässä	Laitteet kommunikoivat käyttäen IP-verkkoa, ja ymmärtävät useita eri protokollia
Laitteet käyttävät langatonta tai langallista yhteyttä	Data siirretään ja sitä käsitellään pilvipalvelussa
Laitteet eivät välttämättä ole yhteydessä internetiin	Pääasiassa laitteet tarvitsevat aktiivisen internetyhteyden
Rajoitettu mahdollisuus integrointiin, koska laitteilla on omat kommunikointistandardit/protokollat	Rajoittamaton mahdollisuus integrointiin, mutta tarvitsevat ratkaisun, jolla hallita yhteyksiä

Tärkeintä on ymmärtää, että vaikka molemmat, M2M ja IOT, viittaavat laitteisiin, jotka kommunikoivat toisten kanssa, niin M2M tarkoittaa käytännössä laitteelta laitteelle kommunikointia. IOT taas viittaa suurempaan kokonaisuuteen, joilla on synergiset ohjelmistopaketit automatisoimaan ja hallitsemaan kommunikointia useiden laitteiden välillä. Niiden operaattoreiden, jotka haluavat tukea IOT:a, pitää asettaa itsensä mahdollisimman myyviksi ja hallita useita yhteyksiä ja vaihtuvia kommunikointiprotokollia, että heidän asiakkaansa voivat nauttia kaikista uusimmista sovelluksista, joita esimerkiksi älytalo voi tarjota. On olemassa joitakin komplikaatioita, kun hallitaan erilaisia standardeja, mutta niin kauan kuin on olemassa IP-yhteys ja oikea ohjelmisto, joka tukee langatonta tai langallista kommunikointia, niin IOT-laitteet kommunikoivat keskenään. IEEE on hiljattain julkaissut luonnoksen langattomasta verkkoprotokollasta 802.11ah. Tämä muutos vuonna 2007 julkaistuun 802.11-standardiin on tarkoitettu asetettavaksi mekanismiksi, joka yhdistää IOT:n käyttämällä matalampaa kaistanleveyttä ja pienempää tehoa, mutta jolla on suurempi tavoittavuus taajuuskaistalla [2].

3 Tietoturvallisuus

COMSEC (communication security)-toimenpiteiden avulla pyritään turvaamaan tieto- ja telejärjestelmissä siirrettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Suomessa on viestintäviraston tehtävä antaa teknisiä määräyksiä ja ohjeita teleyritysten toiminnasta sekä telepäätteiden, -palvelujen ja -verkkojen varustamisesta riittävän tietoturvallisuustason mukaisesti, sekä valvoa että yleistä teletoimintaa harjoittavat teleyri-

tykset täyttävät niille laissa asetetut tietoturvallisuuteen ja viestinnän yksityisyyden suojaamiseen liittyvät velvollisuudet.

Viestintäviraston tehtävänä on valvoa, että kaikki teleyritykset noudattavat viestintämarkkinalakia ja sähköisen viestinnän tietosuojalakia (16.6.2004/516), sekä näiden lakien perusteella annettuja säännöksiä ja määräyksiä, ja että televerkot toteuttavat niitä koskevien teknisten määräysten ja standardien ehtoja. Valvontaa hoidetaan keräämällä eri tavoin tietoa valvonnan kohteista sekä tapauskohtaisilla selvityksillä ja tarkastuksilla [3].

Internet on esimerkki avoimesta tietoverkosta, jossa asioiminen ilman minkäänlaisia suojausmekanismeja on turvatonta. Käyttämällä salaavia yhteyskäytäntöjä ja käyttäjäntodennusmenetelmiä tietoturvaa voidaan parantaa. Salausmenetelmät ja salaavat yhteyskäytännöt vaihtelevat käyttötarkoituksen mukaan, koska mitä suurempaa salausta käytetään, sitä enemmän resursseja se laitteistolta vaatii. Siksi on hyvä määritellä sovellukselle ns. riittävä turvallisuustaso. Pankkipalvelut on hyvä pitää korkeimmalla prioriteetilla, mutta vähemmän kriittisissä sovelluksissa on hyvä pienentää salaustasoa jouhevamman tiedonsiirron aikaansaamiseksi. Salausjärjestelmät voidaan toteuttaa esimerkiksi alemman tason protokollien avulla, jolloin ylemmän tason tiedonsiirrosta (SMTP, FTP, HTTP) riippumatta liikenne kulkee verkossa salattuna.

3.1 Salausprotokollat

Salausprotokollista internetsivujen selauksessa useimmin käytetty on SSL (Secure Socket Layer), jota tänä päivänä tukevat kaikki selaimet. SSL mahdollistaa suojatun yhteyden käytön asiakkaan (Client) koneen ja WEB-palvelimen (Server) välillä. Yhteyden suojaamisen (salauksen) lisäksi SSL mahdollistaa myös kommunikoivien osapuolien tunnistuksen ennen salatun yhteyden muodostamista. Tunnistautuminen tapahtuu varmenteiden avulla siten, että palvelimella on oma palvelinvarmenne, jonka perusteella käyttäjä voi varmistua kommunikoivansa oikean WEB-palvelimen kanssa. Tämän lisäksi SSL tukee myös henkilövarmenteiden hyödyntämistä käyttäjän koneella, ja tätä hyväksi käyttäen käyttäjä voi todistaa oman henkilöllisyytensä WEB-palvelimelle. Toinen hieman kehittyneempi salausprotokolla on TLS (Transport Layer Security), joka on niin sanottu päivitetty versio SSL:stä. Vaikka TLS on eri salausprotokolla, niin yleiskielessä suositellaan puhuttavaksi SSL:stä, koska siitä on kehittynyt niin yleinen termi

salausprotokollalle. Eli tänä päivänä kaikki SSL-sertifikaatit ovat todellisuudessa TLS-sertifikaatteja, joissa on optiona ECC-, RSA- tai DSA-kryptaus. HTTPS (Hyper Text Transfer Protocol Secure) näkyy URL-osoitteessa, kun internetsivu on suojattu SSL-sertifikaatilla. Sertifikaatin tiedot, kuten sertifikaatin myöntäneen viranomaisen ja internetsivun omistavan yrityksen, saa selville, kun painaa selaimen osoiterivillä olevaa lukkokuviota [4].

3.2 Kyberturvallisuus

Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua [5].

Ennen puhuttiin lähes aina tietoturvallisuudesta ja nykyisin tieto-sana on korvautunut lähes samoissa aiheissa kyber-sanalla. Kyberturvallisuus on tietoturvallisuutta sivuava aihe, ja viime aikoina kyber-alkuisia esille nousseita sanoja ovat muun muassa kyberturvallisuus, kyberympäristö, kybersuojaus, kyberpuolustus, kyberhyökkäys ja kybersota. Selkeästi ja yksinkertaisesti kyberturvallisuus-termi on erittäin hankala määritellä, joten kannattaa aloittaa sillä mitä se ei ole. Yleisesti kyberturvallisuus ja -uhat on liitetty internet-verkon ja perinteisen tieto- ja tietoliikennetekniikan toimintojen yhteyteen. Jos asia olisi näin yksinkertainen, voisimme vaihtaa kyber-sanan internet-alkuiseen sanaan. Näin ei voida kuitenkaan tehdä, koska internet ja ICT (Information and Communication Technology)-teknologia on vain pieni osa-alue, jota kyberympäristössä käytetään hyväksi [5; 6].

Esimerkkinä voi ottaa lomamatkan, jolle ollaan menossa lentäen koneella terminaalista. Emme voi kuvitella, että ainoa kriteeri matkan onnistumiseen on se, että lennonjohtajat, lentäjät ja terminaalin henkilökunta on töissä ja hoitavat tehtävänsä. Matkan onnistuminen alkaa jo siitä, että kotona sähköt ovat toiminnassa, kulkuvälineet matkalla terminaaliin toimivat ja saavat sähkönsä tai polttoaineensa. Rautatie tai tiet yleisesti ovat ajokuntoiset ja tietojärjestelmät toimivat [6].

3.3 Kyberturvallisuus vs. tietoturvallisuus

Kyberturvallisuutta lähestyessä pitää ottaa huomioon yhteiskunnallisesta näkökulmasta kokonaisuus, jolla pidetään yhteiskunnan rattaat pyörimässä eli tarkemmin elintärkeiden, kriittisten toimintojen turvaaminen kaikissa olosuhteissa.

Tietoturvallisuus keskittyy pääasiassa ”tiedon” eli datan turvaamiseen kolmesta näkökohdasta

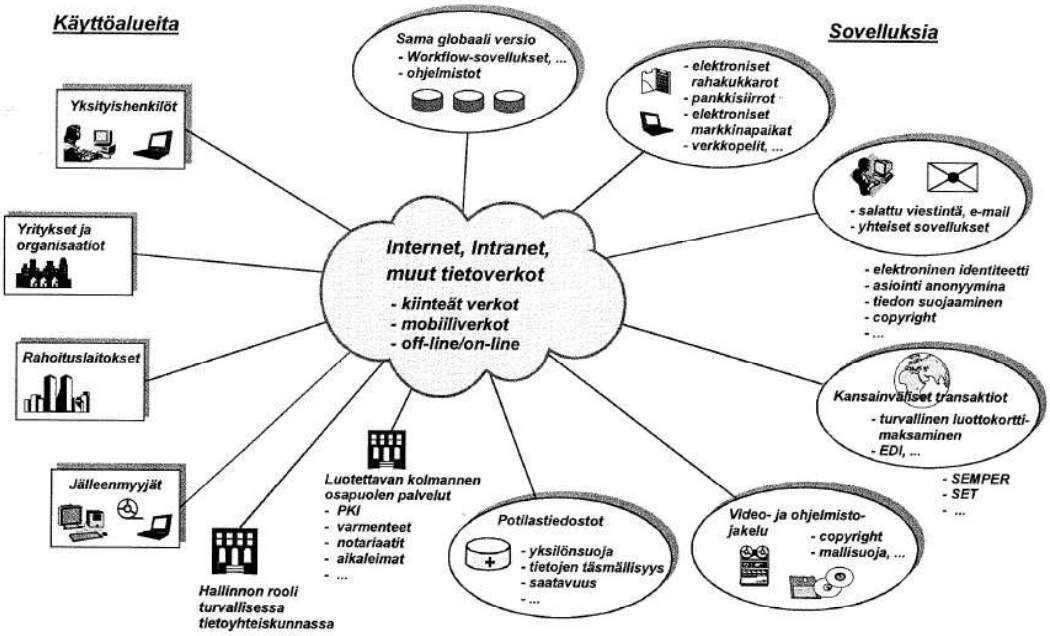
- luottamuksellisuus
- eheys
- saatavuus.

Kyberturvallisuudella taas tarkoitetaan huomattavasti laajempaa kokonaisuutta, jonka yhtenä osa-alueena voidaan pitää myös tiedon turvaamista ja takaamista erilaisissa häiriötilanteissa. Sähkönjakelun ja pankkien sähköisten palveluiden pitää toimia sekä veden virrata – muussa tapauksessa on yhteiskuntamme ongelmissa. Kyber ei juurikaan koske julkishallintoa, koska suurin osa yhteiskuntamme kriittisistä palveluista tuotetaan yritysten toimesta. Tietoturvallisuus on pääasiassa keskittynyt sähköisten tietoaineistojen käsittelyyn, kuitenkaan perinteisiä paperilomakkeita unohtamatta. Kyberturvallisuudessa mennään vastaavasti suojaamaan laajemmin kaikkea infrastruktuuria, jota suojattavan kohteen tuotannon ylläpitäminen vaatii. Tässä ollaan tekemisissä fyysisissä toimitiloissa ja niiden edellyttämissä muissakin kuin vain ICT-teknologian edellyttämissä toiminnoissa [6].

3.4 Kyberturvallisuuden riskejä ja uhkakuvia

Kaikki laitteet, jotka ovat yhteydessä internetiin, kuten tietokoneet ja niiden käyttämät tiedostot sekä ulkoiset tietoverkot ja pilvipalvelut, IOT-laitteet jne. ovat kohteita joihin turvallisuusriskit kohdistuvat. Yleisimpinä järjestelmien uhkatekijöinä voidaan pitää viruksia. Virukset lisääntyvät ja kehittyvät jatkuvasti, mutta niiltä voidaan suojautua virustorjuntaohjelmistoilla sekä palomuureilla. Vaarallisimpia turvallisuuden kannalta ovat järjestelmiin ulkoapäin kohdistuvat hyökkäykset. Käyttäjät eivät ole riippuvaisia pelkästään informaation saatavuudesta, käytettävyydestä ja luotettavuudesta, eivätkä järjestelmistä joissa informaatiota säilytetään ja siirretään, vaan myös näiden järjestelmien

välisten siirtojärjestelmien saatavuudesta ja luotettavuudesta. Tällaiset uhkat sisältyvät verkkoyhtiöillä liiketoimintaan. Kuviossa 1 on esitetty tietoturvan käyttäjiä ja sovelluksia internetissä ja muissa tietoverkoissa.



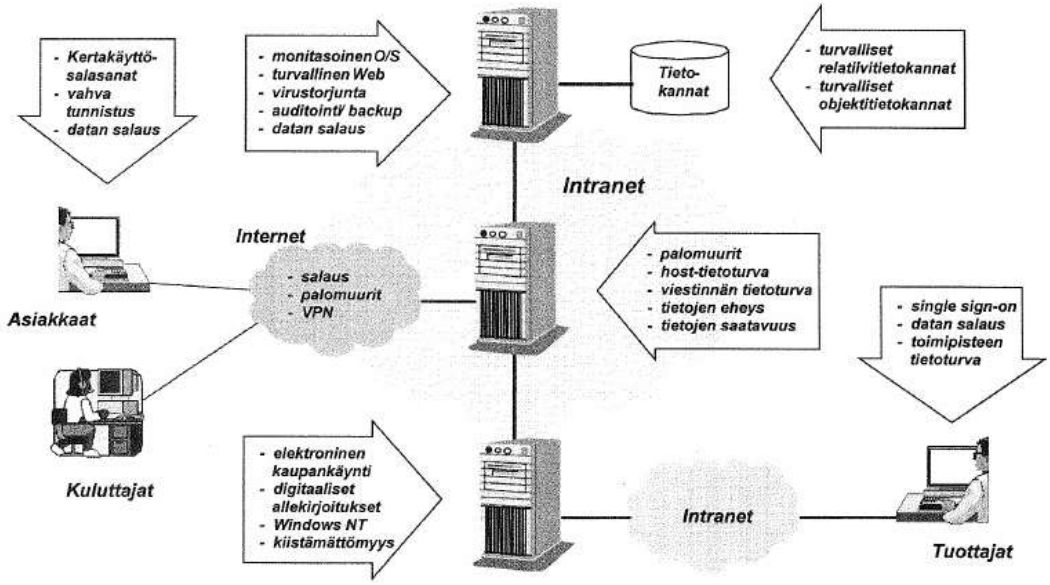
Kuvio 1. Tietoturvan käyttäjiä ja sovelluksia internetissä ja muissa tietojärjestelmissä [7, s. 28].

GSM (Global System for Mobile)-verkkoon perustuvat toisen sukupolven GPRS (General Packed Radio System), kolmannen sukupolven UMTS (Universal Mobile Telecommunications System), neljännen sukupolven LTE (Long-Term Evolution) ja kehitteillä oleva viidennen sukupolven mobiilijärjestelmät ovat osa globaalia infrastruktuuria, joka on kietoutunut yhdeksi isoksi tietoverkoksi ja josta on tullut yksi tietoyhteiskunnan viestintä- ja tiedonsiirron infrastruktuuri. Lähes kaikkiin sovelluksiin ja palveluihin päästään kaikkialta käsiksi ja strategisen tärkeää on turvallisuuden merkitys kaikissa tietoverkoissa [7, s. 32].

Kaikki tietoverkot, kuten internet, intranet, ekstranet ja mobiiliverkot ovat alttiita ulkoisille hyökkäyksille. Ulkoisiin hyökkäyksiin kuuluu muun muassa hakkerointi, vakoilu ja salakuuntelu, yhteyksien katkaiseminen ja laitteisiin kohdistuva vahingonteko. Yleensä järjestelmiin voivat hyökätä kilpailijat, hakkerit tai muut, joita organisaation tietojärjestelmät kiinnostavat. Kuviossa 2 on esitetty, miten yrityksen tietoturva kattaa koko sen toiminnan tietoinfrastruktuurin omista järjestelmistä, verkoista, tietovarannoista ja käyt-

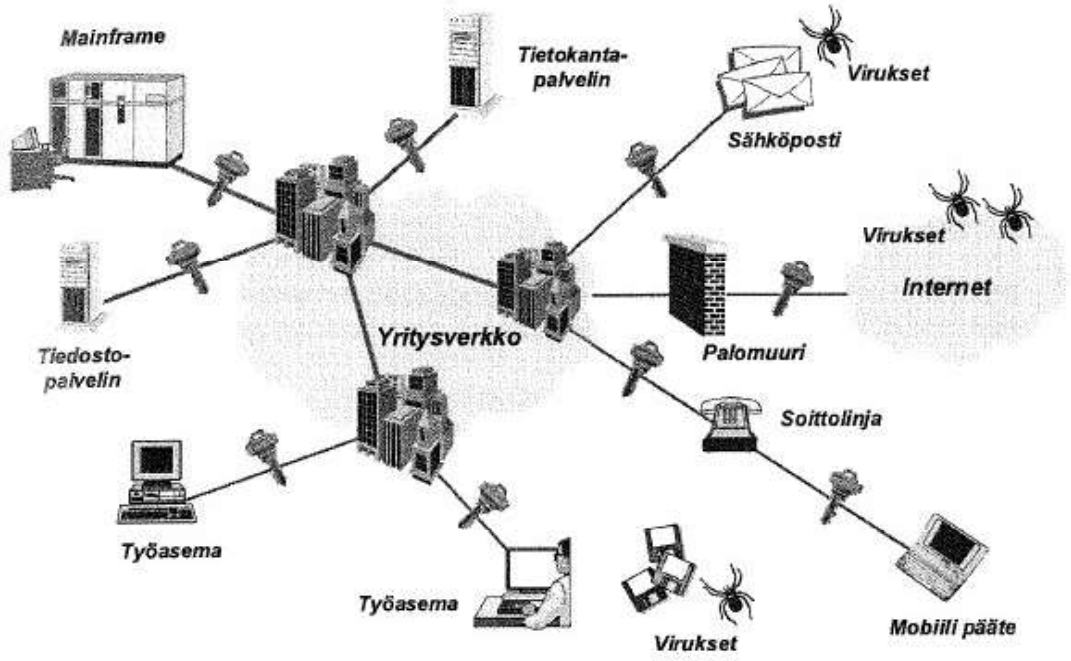
täjistä asiakkaisiin ja tuottajiin saakka. Modernien yrityksien tietoturvakonseptiin kuuluvat muun muassa

- modernit salausmenetelmät
- digitaaliset allekirjoitukset
- julkisen avaimen infrastruktuurit
- VPN (Virtual Private Network)-verkot
- palomuurit
- joustavat access-menetelmät
- virustorjunta
- suojatut tietokannat.



Kuvio 2. Yrityksen tietoturva kattaa koko sen toiminnan tietoinfrastruktuurin omista järjestelmistä, verkoista, tietovarannoista ja käyttäjistä asiakkaisiin ja tuottajiin saakka [7, s. 38].

Kuviossa 3 on kuvattu yrityksen hajautettuja toimintoja, jotka pitää suojata ulkopuolisilta hyökkäyksiltä ja viruksilta. Tähän mahdollisuuden antaa kryptografia, jota käsitellään seuraavassa luvussa. Taulukossa 2 on esitetty yleisimpiä tietoturvariskejä sekä niihin varautumista.



Kuvio 3. Ulkoapäin tulevat tietoturvahyökkäykset ja virusuhkat [7, s. 39].

Taulukko 2. Yleisimmät tietoturvariskit ja niiden vastalääkkeet [7, s. 43].

Tietoturvariski	**Vastalääke**
Laiton tunkeutuminen	Vahva autentikointi ja palomuurit
Tietojen anastaminen yhteydeltä	Salaaminen
Tietojen muuttaminen	Autentikointi, palomuurit, host-koneen suojaaminen, datan eheystyökalut
Sähköpostin sieppaaminen tai väärentäminen	Suojattu sähköposti (esim. PGP, S/MIME)
Tietokonevarkaus	Fyysiset turvatoimenpiteet, laptop-tietojen salaaminen
Palvelun lamauttaminen	Reaaliaikaiset testi- ja monitorointityökalut
Virukset	Virustentorjuntaohjelmistot
Salasanan varkaus	Vahvemmat autentikointimenetelmät
Verkkoon tunkeutuminen	Palomuurit, huolellinen modeemien sijoitus, auditointi, suojattujen modeemien käyttö
Web-palvelimen häiriköinti ja järjestelmään tunkeutuminen Web-palvelimen kautta	Suojatut CGI-skriptit, huolellinen Web-palvelimen konfigurointi ja Web-palvelimen oikeuksien prosessointi
Sisäinen tietoturvarikkomus	Käytön monitorointi, vahva autentikointi, pääsyn valvonnan huolellinen suunnittelu, järjestelmäsuojausten käyttö
Host-koneen ja käyttöjärjestelmän haavoittaminen	Testi- ja monitorointityökalujen käyttö ongelmien havaitsemiseksi ennen kuin tunkeilijat löytävät ne

4 Kryptografia

Kryptografia eli vapaasti tulkittuna salakirjoitustiede viittaa turvallisten viestintämenetelmien tutkimiseen, kehittämiseen ja käyttämiseen kolmansien osapuolien läsnä ollessa, ja se ulottuu aina antiikkiaikoihin asti. Yleisemmästä näkökulmasta se viittaa kolmansien osapuolien vaikutusvallan ylittävien protokollien kehittämiseen ja analysointiin, joissa sovelletaan useaa tietoturvan näkökohtaa, kuten esimerkiksi datan luottamuksellisuutta, eheyttä, autentikointia, kiistämättömyyttä ja samanaikaisuutta. Moderni kryptografiatekniikka on osakokonaisuus eri tieteidenaloja kuten matematiikkaa, tietojenkäsittelytiedettä ja sähkötekniikkaa. Eniten moderni kryptografia pohjautuu matemaattiseen

teoriaan ja tietojenkäsittelytieteen käytäntöön. Kaupankäynnin globalisoituminen ja kilpailun kiristyminen ovat syitä, joiden ansiosta tietoturvallisuudesta on muodostunut verkkoliiketoiminnan avainkysymys [7, s. 63; 8].

4.1 Esihistoria ja klassinen kryptografia

Yksi vanhimmista tiedonsalauskeinoista perustui viestin peittämiseen eli steganografiaan, jossa viestin viejä ajettiin kaljuksi ja viesti kirjoitettiin viejän päähän, ja vasta hiusten kasvettua viestiä pystyi viemään eteenpäin. Hieman nykyaikaisempi esimerkki on Atbash-koodi Caesarin salaaja, jossa selväkielitekstin kirjain korvattiin aina kolmen merkinpäässä olevalla kirjaimella (esim. A → D). Koska Atbash-koodilla on vain yksi avain, niin se on erittäin heikko salakirjoitus. Kehittyneempiä klassisen kryptografian versioita ilmaantui ensimmäisen ja toisen maailmansodan aikana, sotilasviestinnän käyttäessä erilaisia salausmenetelmiä, kuten saksalaisten toisen maailmansodan aikana käyttämä Enigma-salauslaite. Klassisilla kryptografisilla menetelmillä on edelleen oma merkityksensä suljetuissa järjestelmissä, vaikka moderni kryptologia ja tietoverkkojen turvateknologiat perustuvatkin 1970-luvun jälkeen kehitettyihin innovaatioihin (DES, RSA, MD5, X.509 jne.), koska uuden kryptologian kehittäminen perustuu klassiseen kryptologiaan [7, s. 61—63].

4.2 Modernit salausjärjestelmät

Tunnettuja salausalgoritmeja sanomien salaamiseen ovat esimerkiksi DES, 3DES, IDEA, RSA, AES. Olettamalla algoritmien olevan turvallisia, näillä salatut sanomat ovat yhtä salaisia kuin niiden avaimet. Yksi tärkeimmistä kryptografian ongelmista on algoritmien turvallisuuden todistaminen. Vaikka salaus onkin helppo toteuttaa, niin sitä vaikeampi se on toteuttaa turvallisesti. Kryptografian kehitysprosessi on seuraavanlainen, se kehittyy monimutkaisen matematiikan ja iteratiivisen prosessin ohjaamana. Ensin suunnitellaan ja julkaistaan uusi salausmenetelmä ja sitten joku yrittää murtaa sen, ja usein siinä onnistuen. Kaikkien modernien salausmenetelmien luullaan hyvin suurelta todennäköisyydellä olevan murtamattomia, koska ovathan ne kaikki käyneet läpi vuosien kriittiset testit.

> ”Hyvän salausjärjestelmän tulee toteuttaa Kerchoffin periaate, minkä mukaan järjestelmä on varma (salainen), vaikka kaikki sen salaus- ja purkuprosessien yksityiskohdat julkistetaan lukuun ottamatta salaista avainta” [7, s. 65].

Tähän perustuen DES-, RSA- ja AES-algoritmien toimintaperiaatteet on pystytty julkistamaan. Järjestelmän vahvuus piilee sen funktiolohkojen voimakkaassa matemaattisessa epälineaarisuudessa ja yksisuuntaisuudessa.

Kryptografisesti järjestelmä on teoreettisen varma, kun se kestää murrot ja järjestelmän käytettävissä on rajaton määrä laskentakapasiteettia. Tällaista järjestelmää on mahdoton murtaa. Järjestelmä on käytännöllisesti varma, kun se kestää murrot ja järjestelmän käytössä on rajattu määrä laskentakapasiteettia. Tällaista järjestelmää on vaikea murtaa [7, s. 63–66; 8].

4.2.1 DES, 3DES, AES

DES kehitettiin vuonna 1976, ja sen lohkopituus oli 64 bittiä ja avaimen efektiivinen pituus 56 bittiä. Kryptoanalyysillä pyritään murtamaan salaus tuntematta purkuavainta, jota etsitään salausalgoritmien ominaisuuksien ja siirrettävän datan ominaisuuksien perusteella. Ainoa keino murtamisessa on hyväksi käyttää ”raakaa voimaa” ja kokeilla kaikkia mahdollisia avainavaruuden alkioiden kombinaatioita. Tietokoneiden laskentatehon kehityttyä DES-algoritmia ei enää pystynyt pitämään turvallisena ja siitä kehitettiin 3DES. Siinä avaimia oli 3 kappaletta, joten avaimen efektiivinen pituus oli 168 bittiä. Myös 3DES on jo todettu turvattomaksi, ja vuoden 2016 jälkeen sitä ei ole enää esiintynyt. Tästä kehitettiin AES-lohkosalausmenetelmä, joka vuonna 2001 standardoitiin DESin seuraajaksi. AES käyttää 128 bitin lohkoja kolmea eri avainkokoa 128, 196 ja 256 bittiä. Vielä toistaiseksi AES-salausta pidetään murtamattomana, koska 256-bittisellä avaimella salatun AES:n murtaminen veisi kymmeniä vuosia nykyisillä supertietokoneilla. Kvanttitietokone mahdollisesti pystyisi murtamaan suurten lukujen jaollisuuteen perustuvat asymmetriset salakirjoitusmenetelmät nykyistä nopeammin, mutta kvanttitietokoneet ovat vielä hyvin alkeellisella tasolla.

4.2.2 RSA

RSA-salakirjoituksen nimi tulee matemaatikkojen Rivest, Shamir ja Adleman nimien alkukirjaimista. RSA on julkisen avaimen salausalgoritmi, jonka turvallisuus perustuu olettamukseen, jonka mukaan erittäin suurien alkulukujen tulon tekijöihinjako on hankalaa. Sitä voidaan käyttää salaukseen, digitaalisiin allekirjoituksiin, avainten jakeluun ja

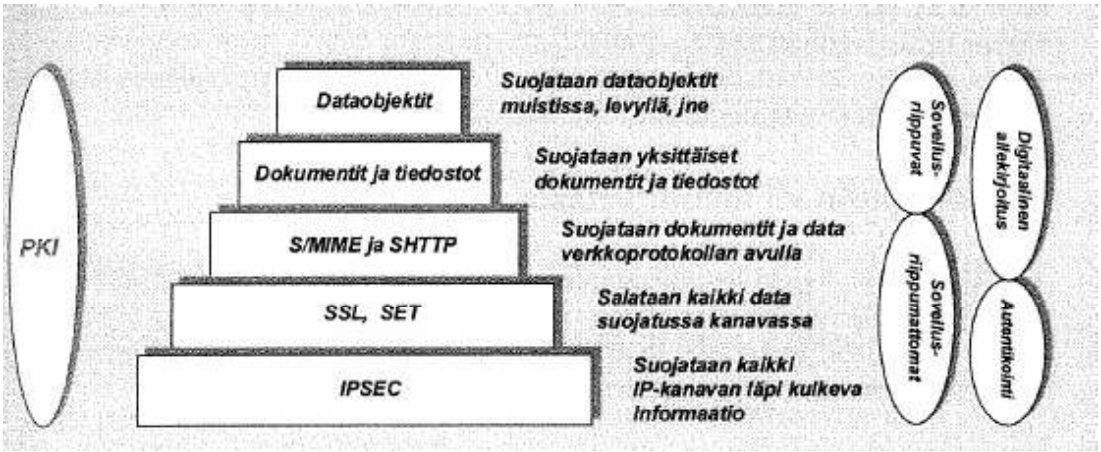
mobiilidatan sekoitukseen. Kryptaus perustuu melko yksinkertaiseen alkulukuteorian tulokseen, ns. Eulerin lauseeseen.

5 Tietoturva-arkkitehtuurit

Tietoliikenneverkot voidaan jakaa kolmeen ryhmään: avoimiin, puoliavoimiin ja suljettuihin verkkoihin. Esimerkkeinä näistä verkkotyypeistä mainittakoon internet (avoin), yritysten lähiverkot (puoliavoin) ja sotilaskäyttöön tarkoitetut verkot (suljettu). Tietoturvanäkökohdat ja kriittiset osa-alueet vaihtelevat verkkotyypeittäin. Tämä koskee myös suojautumismekanismeja, joilla turvauhkien toteutuminen pyritään estämään tai niiden vaikutusta pyritään pienentämään. Internetin perusprotokollia rakennettaessa ei huomioitu riittävästi tietoturvallisuutta, ja osaltaan siksi internetissä asioiminen on sellaisenaan turvatonta. Tietoturvaa voidaan parantaa esimerkiksi käyttämällä salaavia yhteyskäytäntöjä sekä vahvaa todentamista hyödyntäviä käyttäjäntodennusmenetelmiä.

Kuviossa 4 on esitetty näkemys internet/intranet-verkkojen varaan rakentuvasta tietoturva-arkkitehtuurista. Jokaisella toimittajalla on omat tietoturva-arkkitehtuurinsa, jotka rakentuvat liikeidean ja strategian ympärille ja voivat näin poiketa suurestikin toisistaan. Tietoturva-arkkitehtuurin tulee olla joustava ja näkymätön sekä käyttäjäystävällinen, muuten tietoturvasta tulee käytännön haitta eikä turva.

Kerttulan [7, s. 99], mukaan Arkkitehtuuri perustuu standardoituihin kryptoalgoritmeihin ja protokolliin. Julkisen avaimen infrastruktuurin (PKI) palveluja hyödynnetään kaikilla tasoilla avainten ja sertifikaattien myöntämisessä ja hallinnassa. PKI-järjestelmän päällä ovat digitaalista allekirjoitusta ja autentikointia tarjoavat palvelut. Turva-arkkitehtuurin alimmilla tasoilla toteutetaan luotettavia datakanavia ja yritysten VPN-verkkoja esimerkiksi avoimeen internet-ympäristöön. Tietoturva-algoritmit ja protokollat on toteutettu API-ohjelmistolla.



Kuvio 4. Esimerkki tietoverkkojen kryptoteknologiaan perustuvasta kerrostetusta ja avoimesta tietoturva-arkkitehtuurista [7, s. 99].

5.1 PKI

PKI, vapaasti suomennettuna julkisen avaimen infrastruktuuri, on monipuolinen järjestelmä, jonka sovelluksia ovat julkisen avaimen salaaminen, digitaalinen allekirjoitus ja avainten hallinta. PKI-järjestelmiä ja -sovelluksia käyttää hyväkseen esimerkiksi loogisesti turvattu yritysverkko VPN. Yrityksillä on useita tehokkaan julkisen avaimen infrastruktuurin vaatimuksia. Jos käyttäjät eivät pysty hyödyntämään salausta ja digitaalista allekirjoitusta sovelluksissa yksinkertaisesti ja helposti, niin PKI-järjestelmästä ei ole mitään hyötyä. Tärkein PKI:n ominaisuus on läpinäkyvyys, joka merkitsee, että käyttäjän ei tarvitse ymmärtää, miten PKI operoi avaimia ja sertifikaatteja salauksessa ja digitaalisessa allekirjoituksessa [9].

5.2 IPsec-protokolla

IPsec (Internet Protocol Security Architecture) on internetin IETF-järjestön kehittämä standardi. IPsec on joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia. Protokollat tarjoavat salauksen, osapuolten autentikoinnin (todennuksen) ja tiedon eheyden varmistamisen. Suojaus tapahtuu käytännössä host-koneiden välillä eikä host-konetta käyttävien käyttäjien välillä. IPsec- tietoliikenneprotokollat voidaan jakaa kahteen luokkaan:

- protokollat pakettivirtojen turvaamiseen (ESP)
- avaintenvaihtoprotokolla turvattujen pakettivirtojen muodostamiseen (IKE).

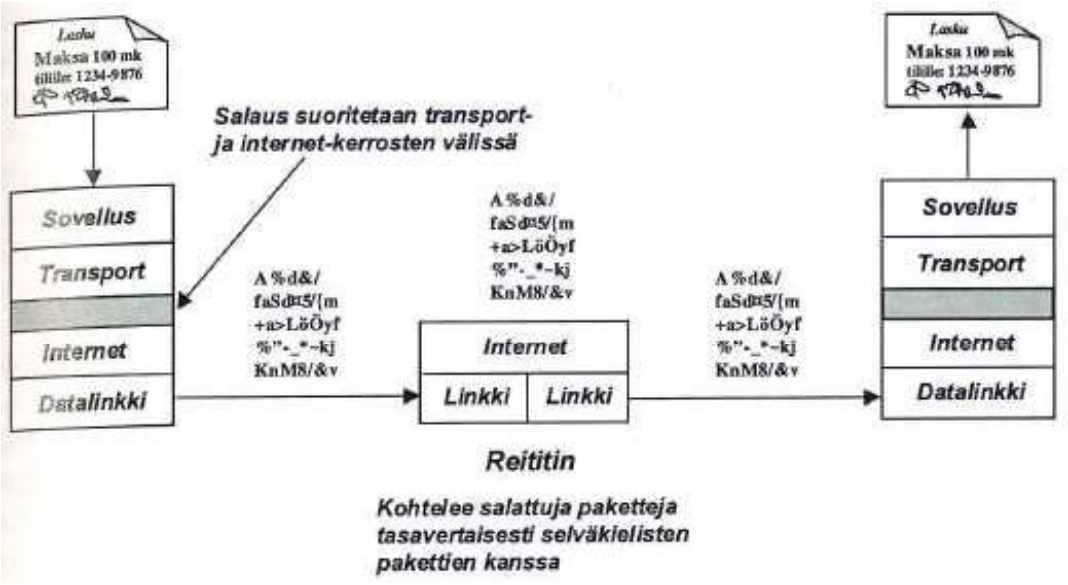
Pakettivirtojen turvaamiseen on tarjolla kaksi vaihtoehtoista protokollaa, jotka ovat AH (Authentic Headers) ja ESP (Encapsulating Security Payloads). ESP on tavallisempi, ja sitä käytetään pakettivirtojen salaamiseen. AH-protokolla on harvemmin käytetty, ja sen tehtävä on tarjota autentikointi ja eheys, mutta ei kuitenkaan luottamuksellisuutta.

IPSec-protokollan kanssa käytettäväksi suositeltu avaintenvaihtoprotokolla on IKE (Internet Key Exchange), joka koostuu ISAKMP-, Oakley- ja SKEME-protokollien yhdistelmästä. IKE:stä tällä hetkellä yleisessä käytössä on IKEv2, mutta laitteiden kehittyessä myös tästä ollaan kehittämässä uutta versiota, jota ei ole vielä julkaistu.

IPSec on määritelty pakolliseksi IPv6:een ja se on mahdollista sovittaa myös IPv4:ään. Verkkotason IPSec-suojaus ei vaikuta sovellusohjelmiin, ja IPSec-paketteja voivat käsitellä jo käytössä olevat reitittimet ja reitittävät host-koneet. (Kuvio 5.)

Kuvio 5. IPSec-salauksen paketin perusformaatti [7, s. 220].

Siirron aikana IPSec salaa ja sinetöi kuljetus- ja sovellusdatan. Myös verkko-otsikon eheys salataan. IP-reitittimet voivat reitittää salattuja IPSec-sanomia vastaanottavaan host-koneeseen saakka, koska verkko-otsikko on selväkielistä, kuvio 6 [7, s. 220].



Kuvio 6. IPSec-suojaus on ”läpinäkyvää” internet-sovelluksille ja – reitittimille [7, s. 221].

IPSEC-protokollat toimivat OSI-mallin verkkokerrostasolla, minkä vuoksi ne soveltuvat myös muiden kuin TCP-pohjaisten protokollien suojaamiseen. Pääasiassa tämä tarkoittaa UDP-pohjaisia sovelluksia, ICMP-kontrolliviestejä ja reitityksessä ja tunneloinnissa käytettyjä IP-protokollia. Kuljetuskerroksen protokolliin (kuten SSL/TLS:ään) verrattaessa haittapuolena IPSec-prokollassa voidaan pitää sitä, että IPSec-protokollien pitää pystyä hallitsemaan myös vakaus- ja fragmentoitumisongelmat, jotka tyypillisesti hoidetaan korkeammalla tasolla, TCP- eli kuljetuskerrostasolla. Reitittimet eivät huomioi ylimääräisiä IPSec-otsikoita eivätkä sovellukset näe IPSec-kryptopalveluja. IPSec on suunniteltu IP-pakettien luottamuksellisuutta sekä väärennysten havaitsemista varten. IPSec määrittelee kaksi optionaalista pakettiotsikkoa, kummallekin suojaustavalle (turvapalvelulle) oman. Otsikot sisältävät numeroarvon, jota kutsutaan SPI-parametriksi (Security Parameter Index). Host-kone käyttää SPI-parametriä kryptoavainten ja niiden käytön tunnistamiseen. IP-paketti voi sisältää yhden tai molemmat otsikot riippuen tarvittavasta turvapalvelusta. Yleensä implementoidaan molemmat [7, s. 221].

IPSec-otsikot ovat seuraavat:

- Autentikointiotsikko (Authentication Header, AH). AH sisältää eheyden tarkistusinformaatiota, jolla voidaan tarkistaa, onko paketin sisältöä väärennetty tai muutettu matkalla läpi epäluotettavan verkkoyhteyden. AH-otsikko sisältää tätä varten kryptografisen tarkistussumman (Checksum). Tarkistussumma tuottaa salaista avain informaatiota, joten ulkopuolinen murtautuja ei pysty laskemaan toista tarkistussummaa, mikä osoittaisi sisällön aitouden.

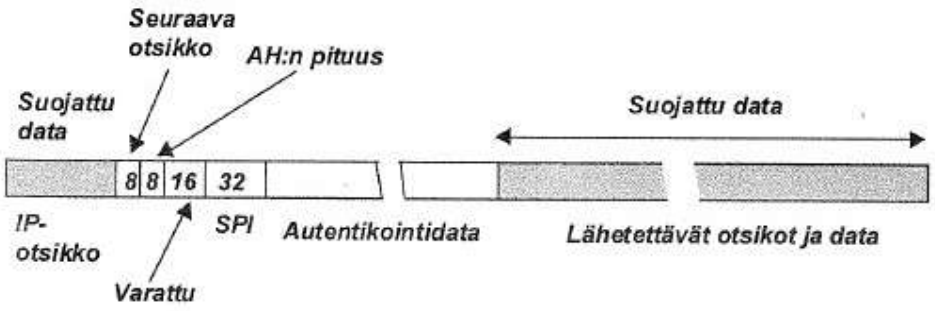
- Yleisemmin käytetty koteloitu salattu data (Encapsulating Security Payload, ESP). ESP salaa paketin loppuosan datasisällön, joten sisältöön ei päästä käsiksi matkalla. ESP-otsikon formaatti vaihtelee sen mukaan, mitä salausalgoritmiä käytetään. Kaikissa tapauksissa käytettävä salausavain valitaan parametrin SPI avulla.

Kummankin IPSec-suojaukseen pyrkivän host-koneen tulee muodostaa aluksi turvayhteys toinen toiseensa. Turvayhteys määrittelee, mitä ja miten IPSec-suojausta käytetään, eli mitä turvapalvelua milloinkin käytetään, miten salaus ja/tai autentikointi suoritetaan ja mitä avaimia tulee käyttää. Turvayhteys muodostetaan kyseessä olevan IP-paketin vastaanottajan otsikon ja pakettiotsikon SPI-parametrin avulla [7, s. 221–222].

5.2.1 IPSec-autentikointi

IPSec-protokollan IP-paketin AH-otsikko sisältää paketin sisällöstä lasketun kryptografisen tarkistussumman. AH sijoitetaan IP-otsikon ja minkä tahansa sitä seuraavan pakettisisällön väliseen pakettiin. Pakettien datasisältöön ei tarvitse tehdä mitään muutoksia. Suojaus on kokonaan AH-otsikossa.

Kuviossa 7 on kuvattu IP-paketin AH-otsikon muoto ja sisältö. AH:n muoto on hyvin yksinkertainen. Ensimmäinen merkki identifioi seuraavan protokollaotsikon tyypin ja paikan ja AH voidaan jopa ylittää autentikoimatta sitä. SPI kertoo vastaanottajalle, mikä turvayhteys koskee tätä otsikkoa. Otsikon loppuosa muodostuu 32 bitin merkeistä, mikä sisältää mainitun kryptografisen tarkistussumman. Tarkistussumman tai hash-funktion yksityiskohtainen muoto ja sisältö riippuu siitä, mitä algoritmia tällä turvayhteydellä käytetään (SHA, MD5).

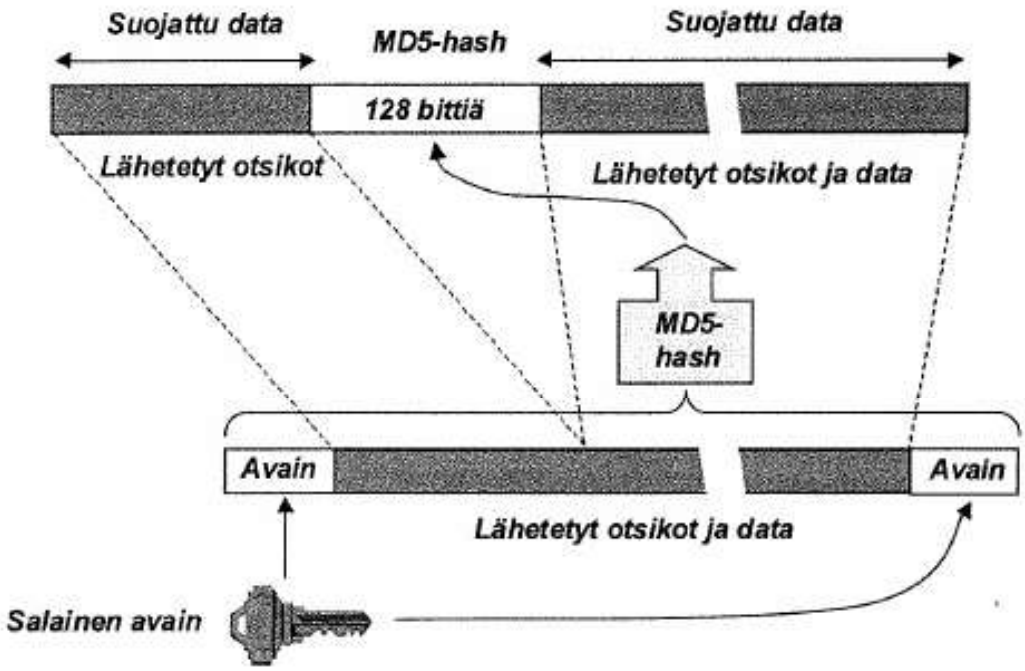


Kuvio 7. IPSec-protokollan AH-otsikon muoto ja sisältö [7, s. 223].

Kryptografinen tarkistussumma määrätään paketin IP-otsikosta yhdistettynä AH:ta seuraavilla otsikoilla. Sisällyttämällä IP-otsikko tarkistuslaskentaan, AH voi havaita kaikki paketin osoiteinformaatioon kohdistuneet muutokset tai yritykset ohittaa ne itse. Vastaanottava host-kone suorittaa vastaavat laskelmat ja todentaa tarkistussumman. Kaikkien kenttien arvot, jotka eivät vastaa summaa, asetetaan nolliksi. Tarkistussumman laskentaan käytetään SPI-parametriin yhdistettyä avainta. Jos tarkistussumman tulos ei vastaa AH-otsikossa vastaanotettua arvoa, paketti hylätään. IPSec-autentikoinnin hash-funktion oletusarvona on MD5 (salainen avain ja 128-bittinen tiiviste), jonka tulee sisältyä kaikkiin IPSec-implementaatioihin. Protokolla jättää salaisen avaimen pituuden avoimeksi. Kaksi host-konetta voi liikennöidä keskenään, jos ne sopivat avaimen pituudesta, sisällöstä ja bittien järjestyksestä [7, s. 222–223].

IPSec-autentikoinnin yleinen periaate on esitetty kuviossa 8. Periaate on sama kuin muussakin normaalissa hash-funktiota käyttävässä autentikoinnissa, sillä erotuksella, että hash-funktio laskee tiivisteen salatusta datasta. Hyökkääjä ei pysty toistamaan hash-laskentaa, koska hänen pitää ensiksi purkaa data, josta tiiviste määrätään.

SPI-parametriin liittyvä salainen avain liitetään suojattuun dataan kahdesti. Analyysit ovat osoittaneet, että tämä konsepti kestää hyökkäyksiä enemmän kuin ainoastaan yhden avaimen käyttö. Tämän jälkeen lasketaan MD5-tiiviste kombinoidusta datasta. Tästä syntyvä 128 bitin tiiviste sijoitetaan paketin AH-otsikkoon. Vastaanottaja todentaa tiivisteen konstruoimalla oman hash-arvon käyttämällä samaa salaista avainta, mikä oli liitetty suojattavan datan alkuun ja loppuun. Jos vastaanotettu sanoma on aito, AH-otsikossa vastaanotettu ja perillä laskettu tiiviste ovat samat ja päinvastoin.



Kuvio 8. MD5-tiivisteellä varustettu IPSec-autentikointi [7, s. 224].

5.2.2 IPSec-salaus

IPSec ESP (Encapsulating Security Payload) on IPSec-protokollasovelluksen jäsen, joka tarjoaa alkuperäntodennuksen (autentikoinnin), tietojen eheyden hajautusfunktion avulla ja luottamuksellisuuden IP-pakettien kryptografisella salauksella. ESP tukee myös pelkkää salaus- tai pelkkää autentikointikonfiguraatiota, mutta salaus ilman autentikointia ei ole tyypillinen ratkaisu. Toisin kuin AH, kuljetustilassa ESP ei tarjoa eheyttä ja autentikointia koko IP-pakettiin, mutta ”tunnelitilassa”, jossa koko alkuperäinen IP-paketti on kapseloitunut uudella pakettiotsikolla, ESP tarjoaa suojauksen koko IP-paketille. Normaaliolosuhteissa ESP sijaitsee AH-otsikon sisällä. Paketin generoima host-kone kryptaa datan käyttämällä turvayhteydellä valittua algoritmia ja avainta, ja asettaa SPI-parametrin ESP-otsikkoon. Autentikointi suoritetaan tämän jälkeen paketin salatusta sisällöstä.

Vastaanotetussa datassa prosessoidaan ensin AH, jos se on käytössä. Jos salattua dataa on ”peukaloitu” matkalla, AH-prosessi havaitsee tämän ja paketti hylätään. Tämän jälkeen host-kone ottaa käyttöön ESP-otsikkoon liitetyn avaimen ja kryptoalgoritmin ja purkaa salauksen.

Oletuksena käytetään AES-algoritmin CBC-moodia. Moodi käyttää vähintään 128 bitin salausavainta. Data salataan peräkkäin 64 bitin lohkoina.

IPSec-protokollaa voidaan käyttää jompaankumpaan seuraavista:

- yhteydenpitokanavan turvaamiseen, jolloin kone/koneita voi olla useita, tai vaikka kokonainen lähiverkko, joiden tietoliikenne laitetaan kulkemaan yhden pisteen (palomuurin) kautta, joka hoitaa lähtevän liikenteen salauksen ja tulevan liikenteen purkamisen.
- pakettiliikenteen turvaamiseen lähettäjältä vastaanottajalle, eli niin kutsuttu (point to point), jolloin salauksen vaatimat prosessoinnit hoitavat päätepisteiden tietokoneet.

IPSec-protokollaa voidaan myös käyttää VPN:n eli näennäisen yksityisverkon rakentamiseen molemmilla tavoilla. Pitää kuitenkin huomioida, että saavutettava tietoturva eroaa näiden kahden mallin välillä. VPN on yleistynyt huomattavasti, mutta päästä-päähän-yhteyksien yleistyminen on ollut erittäin hidasta. Kun siirretään luottamuksellista tietoa, niin on syytä käyttää lisäksi erillisratkaisuja, kuten SSL/TLS-protokollaa.

5.3 SSL/TLS-protokolla

SSL-protokolla on alun perin Netscapen vuonna 1994 kehittämä salausmenetelmä Web-käyttöön. Nykyisin SSL on korvattu kehittyneemmällä TLS-salausprotokollalla, joka on niin sanottu päivitetty versio SSL:stä, ja se otettiin käyttöön vuonna 1999. Vaikka TLS on eri salausprotokolla, niin yleiskielessä suositellaan edelleen puhuttavaksi SSL:stä, koska siitä on kehittynyt niin yleinen termi salausprotokollasta. Internetsivustot voivat käyttää TLS-protokollasuojaa kaikkeen kommunikointiin palvelimen ja selaimen välillä. TLS-protokolla pyrkii ensisijaisesti tarjoamaan yksityisyydensuojaa kahden tai useamman kommunikaatiosovelluksen välillä. Kun TLS varmentaa asiakkaan ja palvelimen välisen yhteyden, sillä saadaan aikaan yksi tai useampia seuraavista ominaisuuksista [10].

- Yhteys on yksityinen ja turvallinen, koska tietojen lähetykseen käytetään symmetristä salausta. Symmetrisen salauksen avaimet luodaan ainutkertaisesti jokaiselle yhteydelle ja se perustuu yhteiseen salaukseen, joka on neuvoteltu (TLS-kätelty) istunnon alussa. Palvelin ja asiakas neuvottelevat yksityiskohdista, eli mitä salausalgoritmiä ja kryptografista avainta käytetään ennen tietojen ensimmäisen tavun lähettämistä. Yhteisen salauksen neuvotteleminen on sekä turvallista että luotettavaa.

- Yhteyksien osapuolien henkilöllisyys voidaan todentaa käyttämällä julkisen avaimen salausta. Tämä todennus voidaan tehdä valinnaiseksi, mutta se vaaditaan yleensä ainakin yhdelle osapuolelle, yleensä palvelimelle.

- Yhteys on luotettava, koska jokainen lähetetty sanoma sisältää sanoman eheyden tarkistuksen käyttäen sanoman todennuskoodia, jotta voidaan estää havaitsematon menetys tai tietojen muuttaminen lähetyksen aikana.

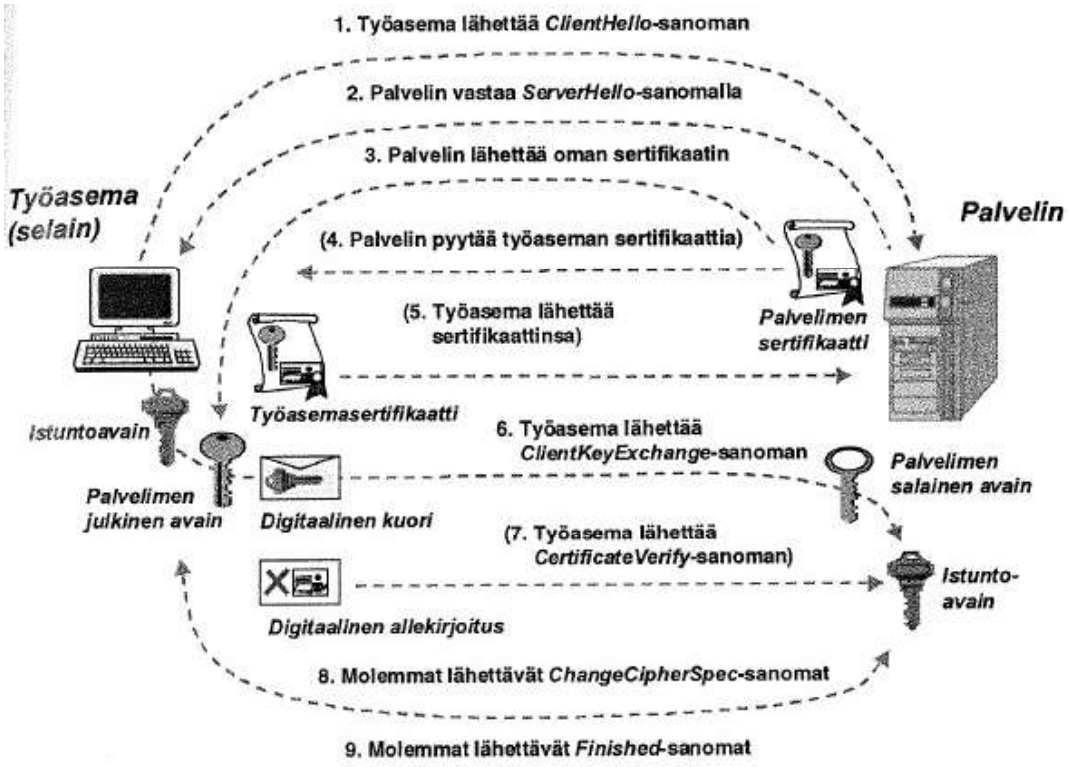
Edellä mainittujen ominaisuuksien lisäksi TLS:n varovainen konfigurointi voi tarjota myös muita tietosuojaan liittyviä ominaisuuksia, kuten esimerkiksi salassapitovarmuutta siten, että myöhemmällä salausavaimella ei voida purkaa aiempia TLS-viestejä. TLS tukee monia eri metodeita vaihtaa avaimia, salata tietoja ja tunnistaa viestien eheys. Tämän tuloksena TLS:n turvallinen konfigurointi pitää sisällään useita konfiguroitavia parametrejä, joten ainoastaan osa ominaisuuksista on kuvattu yllä olevassa luettelossa. TLS-protokollaan kuuluu kaksi kerrosta: TLS-tietue ja TLS-kättelyprotokollat.

5.3.1 SSL/TLS-protokollan kuvaus

Asiakas-palvelin-sovellukset käyttävät TLS-protokollaa kommunikointiin verkon välityksellä, mikä on suunniteltu estämään salakuuntelua ja luvattomuutta. Koska sovellukset voivat kommunikoida toistensa kanssa joko TLS:n kanssa tai ilman sitä, niin on välttämätöntä, että asiakas ilmoittaa palvelimelle TLS-yhteyden muodostamisesta. Yksi tärkeimmistä tavoista ilmoittaa palvelimelle on käyttää eri porttinumeroa TLS-yhteyksille, esimerkiksi portti 443 HTTPS:lle. Toinen mahdollinen keino on, että asiakas tekee protokollakohtaisen pyynnön palvelimelle vaihtaa yhteys TLS:ksi, esimerkiksi tekemällä STARTTLS-pyynnön sähköposti- tai uutisprotokollan käytön yhteydessä.

Kun asiakas ja palvelin ovat suostuneet käyttämään TLS:ää, he neuvottelevat yhteyden kättelyn avulla. Protokollat käyttävät kättelyä epäsymmetrisen salauksen avulla, jotta ei ainoastaan luoda salausasetuksia, vaan myös istuntokohtainen jaettu avain, jonka avulla viestintä salataan käyttäen symmetristä salausta. Tämän kättelyn aikana

asiakas ja palvelin sopivat erilaisista parametreistä, joita käytetään yhteyden salaamiseen. Tämä prosessi on kuvattu kuviossa 9.



Kuvio 9. SSL protokolla on 9-vaiheinen neuvottelu, jossa autentikoidaan molemmat osapuolet ja luodaan istuntoavain [7, s.299].

Tämän jälkeen kättelyprosessi loppuu ja sekä asiakas että palvelin luovat premaster-avaimesta istuntoavaimen (master-avain) salatakseen tulevan liikenteen symmetrisesti molempiin suuntiin. Jos jokin kuviossa mainituista vaiheista epäonnistuu, TLS-kättely epäonnistuu ja yhteyttä ei luoda.

TLS/SSL-protokolla ei sovi suoranaisesti millekään OSI-mallin tai TCP/IP-mallin yksittäiselle kerrokselle. TLS toimii luotettavan esimerkiksi TCP-protokollan päällä, mikä merkitsee, että se on kuljetuskerroksen yläpuolella. Se tarjoaa salausta korkeampiin kerroksiin, mikä on tavallisesti esitystapakerroksen tehtävä. Kuitenkin sovellukset yleensä käyttävät TLS:ää ikään kuin se olisi kuljetuskerroksella, koska TLS:ää käyttävät sovellukset joutuvat aktiivisesti hallitsemaan aloittavia TLS-kättelyjä ja vaihdettujen autentikointisertifikaattien käsittelyä [10].

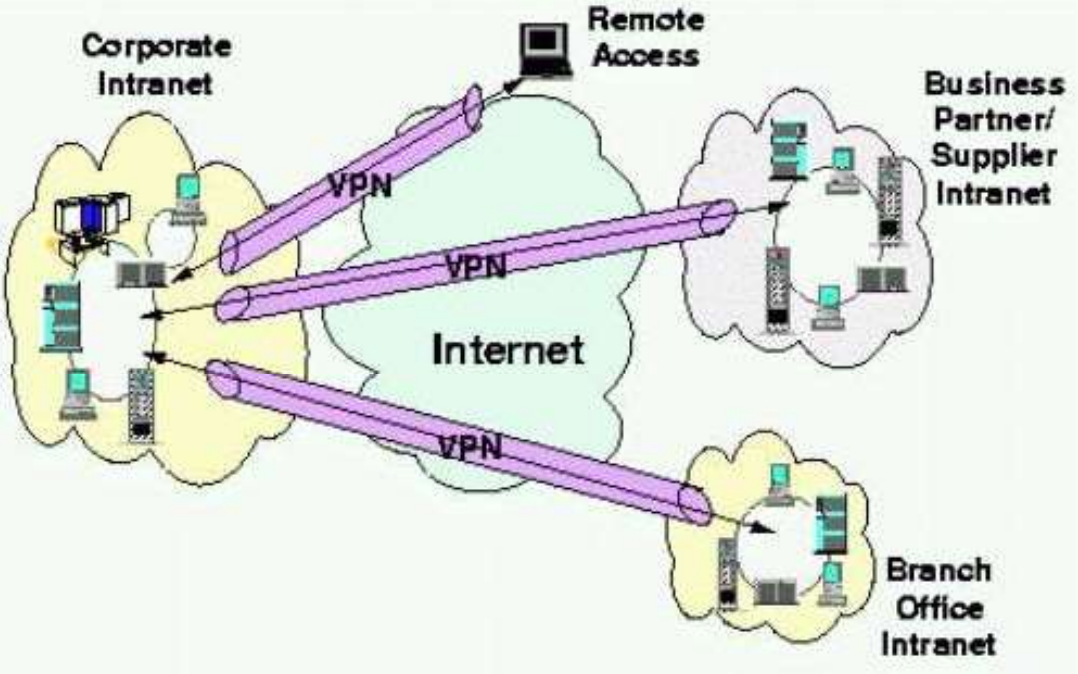
5.3.2 SSL/TLS-protokollan edut ja haitat

Etäyhteyden ottaminen ei sido paikkaan eikä laitteistoon. Yhteys on mahdollista luoda mistä tahansa, kahvilasta, kirjastosta, työkoneelta tai kotikoneelta. Protokollan käyttö ei vaadi kuin selaimen, koska SSL/TLS-protokollaa tukevat kaikki selaimet. Protokollaa kehitetään koko ajan ja siitä syystä on hyvä pitää huolta ohjelmistopäivityksistä, että käytössä on aina uusin versio. Kaikki yhteydet eivät ole suojattuja, koska SSL/TLS-suojauksen vaatima 9-vaiheinen kättelyprosessi vaatii suorituskykyä, jota mobiililaitteistolla on rajoitetusti, sekä tähän toimenpiteeseen kuluva aika näkyy myös palvelun/sivun vasteajassa.

Tietoturvallisuuden kannalta yhteydenottoja kaikilta koneilta, varsinkaan julkisista paikoista ei suositella, vaikka se onkin mahdollista. Koneelle jää aina merkintä tapahtumista, sekä käyttäjä saattaa epähuomiossa ladata arkaluontoista dataa koneelle tarkoituksena siirtää se esimerkiksi pilvipalveluun tai muistitikulle, eikä muistakaan poistaa sitä julkiselta koneelta. Varminta olisi olla tallentamatta/lataamatta dataa tuntemattomille koneille ollenkaan. Kannettavan omistajan, joka käyttää etäyhteyttä, on syytä huolehtia tietokoneen tai mobiililaitteen suojauksesta. Tällä ainakin hidastetaan varkaan pääsemistä käsiksi tietoihin.

6 Virtuaalinen yksityinen verkko

VPN (Virtual Private Network), vapaasti Suomennettuna ”Virtuaalinen yksityinen verkko”, tarkoittaa virtuaalista lähiverkkoa (VLAN). VPN laajentaa yksityisen verkon julkisen verkon kautta ja antaa käyttäjille mahdollisuuden lähettää ja vastaanottaa tietoja yhteisten tai julkisten verkkojen kautta ikään kuin laitteisto olisi yhteydessä yksityisessä verkossa. VPN:n kautta kulkevat sovellukset voivat siten hyötyä yksityisen verkon toimivuudesta, turvallisuudesta ja hallinnasta. VPN pystytään toteuttamaan joko ohjelmistolla, laitteistolla tai niiden yhdistelmällä toteutetulla ratkaisulla. Kaikille käyttöjärjestelmille on tarjolla sekä kaupallisia että ilmaisia VPN-ohjelmistoja. Laitteistoratkaisut ovat aina suositeltavampia, koska niiden avulla voidaan suojata isojakin kokonaisuuksia. Ohjelmistopohjaiset ratkaisut eivät välttämättä ole suurissa kokonaisuuksissa niin luotettavia kuin laitteistot, ja niiden päivitys voi aiheuttaa ongelmia [11]. Kuviossa 10 on esimerkki VPN-tunneloinnista.



Kuvio 10. VPN-tunneli on luotu internetin ”päälle” toimisteiden välille. Käyttäjä(t) pääsevät toisen toimipisteen lähiverkkoon käyttämällä tunneloitua yhteyttä [12].

VPN:n avulla mahdollistetaan turvallisen yhteyden luominen avoimien (turvattomien) verkkojen, kuten internetin yli. VPN:t voivat sallia esimerkiksi työntekijöiden tai liikekumppanien turvallisen pääsyn yrityksen intranetiin toimiston ulkopuolelta. Niitä käytetään yhdistämään toisiinsa maantieteellisesti erillään olevat toimistot, jotka muodostavat yhtenäisen verkon. Vaikka käyttäjät olisivatkin fyysisesti kaukana toisistaan, he näkevät toisensa aivan kuin he olisivat samassa lähiverkossa. Yksittäiset internetin käyttäjät voivat varmistaa liiketoimintansa VPN:llä, kiertää geologisia rajoituksia ja sensuuria tai muodostaa yhteyden proxy-palvelimiin henkilökohtaisen identiteetin ja sijainnin suojelemiseksi, jotta he voivat pysyä nimettöminä avoimessa internetissä. Jotkin internet-sivustot estävät pääsyn, jos käyttää VPN-tekniikkaan perustuvaa yhteyttä estääkseen geologisten rajoituksien kiertämisen. Tästä syystä myös monet VPN-palvelujen tarjoajista ovat kehittäneet tekniikoita näiden esteiden poistamiseksi [11].

6.1 Tekniikka

VPN-tekniikka perustuu tunnelointiin (tunnel). VPN luodaan muodostamalla virtuaalinen piste-piste-yhteys (P2PP) käyttämällä olemassa olevia yhteyksiä, virtuaalisia tunnelointiprotokollia tai kryptologioita. VPN:ssä siirrettävän tiedon suojaamiseen käytetään salausta, joka estää verkossa välitettävän tiedon paljastumisen kolmansille osapuolille. Salauksen lisäksi VPN-ratkaisut mahdollistavat keskustelevien osapuolien vahvan todennuksen. VPN-ratkaisut käytännössä tarjoavat julkisen verkon kautta laajakaistaverkon (WAN) edut. Yleisesti käytössä olevia VPN-protokollia ovat IPSec, L2TP, PPTP sekä VPLS. VPN-verkot voivat olla joko kaukoyhteys (jota käytetään hyödyksi M2M-yhteydessä) tai kahden erillään olevan lähiverkon yhteen liittäminen. Kuljetusprotokolla on tavallisimmin TCP-protokolla. [11]

VPN-järjestelmät voidaan luokitella seuraavasti:

- tunnelointiprotokolla, jota käytetään tietoliikenteen tunneloinnissa
- tunnelin liiitäntäpisteen sijainti, esimerkiksi asiakasrajapinnalla tai verkko-operaattorin rajalla
- yhteyden topologian mukaan, esimerkiksi sijaintipaikasta - sijaintipaikkaan tai lähiverkosta – lähiverkkoon
- turvatasojen mukaan
- OSI-kerrosten mukaan, kuten 2-tason piirit tai 3-tason verkkoyhteydet
- samanaikaisten yhteyksien lukumäärän mukaan.

VPN:n suurimpana vahvuutena on, että se käyttää jo olemassa olevia yhteyksiä. Riittää kun VPN-asiakkaalla on yhteys internetiin. VPN on huomattavasti halvempi ja joustavampi vaihtoehto kuin vuokrakaapeliyhteys.

6.2 VPN-protokollan turvamekanismit

VPN-verkot eivät voi tehdä verkkoyhteyksiä täysin anonyymeiksi, mutta ne voivat yleensä lisätä yksityisyyttä ja turvallisuutta. Yksityisten tietojen paljastamisen estämiseksi VPN-verkot sallivat tyypillisesti vain tunnistetun etäyhteyden käyttäen tunnelointiprotokollia ja salaustekniikoita. VPN-suojausmalli tarjoaa seuraavat edut:

- luottamuksellisuus, vaikka verkkoliikennettä pakettitasolla pääsisi ”nuuskimaan”, hyökkääjä näkee ainoastaan salattuja tietoja
- tietojen lähettäjän todennus, estää luvattomat käyttäjät pääsemästä VPN-palveluun
- viestin eheys kaikkien lähetettyjen viestien väärentämisen havaitsemiseksi.

Turva VPN-protokolla sisältää seuraavat ominaisuudet:

- IPSecin joka alun perin kehitettiin suositukseksi IPv6:een, mutta nykyisin se on määritelty pakolliseksi. Tämä standardipohjainen tietoturvaprotokolla on myös laajasti käytössä IPv4:ssa ja kerroksen 2 tunnelointiprotokollan kanssa. Se on suunniteltu täyttämään useimmat turvallisuustavoitteet, kuten todennuksen, eheyden ja luottamuksellisuuden.
- Liikennetason suojauksen (SSL/TLS), joka voi tunneloida koko verkon liikenteen, (esimerkiksi OpenVPN) tai suojata yksittäisen yhteyden. VPN-yhteyden voi muodostaa paikoista, joissa IPSec:in kanssa tulee ongelmia, kuten NAT:in (Network Address Translation) ja palomuurien kanssa SSL/TLS:n avulla toteutettuna
- DTLS:n (Datagram Transport Layer Security), jota käytetään (Ciscon AnyConnectVPN:ssä ja OpenConnectVPN:ssä) ongelmien ratkaisuun SSL/TLS tunnelointiin UDP:n kautta.
- SSH (Secure Shell) VPN- OpenSSH tarjoaa VPN-tunneloinnin varmistaakseen etäyhteydet verkkoon tai verkkoyhteyksiin, OpenSSH-palvelin tarjoaa rajoitetun määrän rinnakkaisia tunneleita. Tämä ei kuitenkaan tue henkilökohtaista todennusta.

6.3 VPN-protokollan autentikointi

Tunnelin päätepisteet on todennettava ennen kuin varmistetaan VPN-tunnelit. Käyttäjille luodut etäyhteysvarmistukset voivat koostua salasanoista, biometriikasta, redusoiduista salasanoista tai muista salausmenetelmistä. Verkosta-verkkoon-tunnelit käyttävät yleensä salasanoja tai digitaalisia sertifikaatteja. Avain voidaan tallentaa pysyvästi, jotta tunneli on muodostettavissa automaattisesti ilman järjestelmänvalvojan toimia.

6.4 Reititys

Tunnelointi-protokollat voivat toimia pisteestä-pisteeseen (P2P)-topologiassa, vaikka tätä ei teoriassa pitäisi nimittää VPN:ksi, koska VPN:n määritelmän mukaan sen odote-

taan tukevan mielivaltaisia ja muuttuvia verkkosolmukohtia. Koska useimmat reitittimien toteutukset tukevat ohjelmiston määrittämää tunnelikäyttöliittymää, asiakaslähtöiset VPN:t ovat usein yksinkertaisesti tunnettuja tunneleita, jotka käyttävät tavanomaisia reititysprotokollia.

6.5 VPN:t reitittimissä

VPN-verkkojen käytön lisääntyessä monet ovat alkaneet käyttää VPN-yhteyttä reitittimissä lisäämään suojausta ja käyttämään tiedonsiirron salaamiseen kryptografisia tekniikoita. Kotikäyttäjät käyttävät tyypillisesti VPN-verkkoja reitittimissään suojaamaan laitteita, kuten äly-TV:tä tai pelikonsolia, joissa voi käyttää VPN-clientia. Yrityksillä tämä yleistyy sitten, kun IOT yleistyy ja koneita sekä antureita on verkossa. Siksi monet reitintinvalmistajat tarjoavat reitittimiä sisäänrakennetuilla VPN-clienteilla. Jotkut käyttävät avoimen lähdekoodin laiteohjelmistoja (kuten DD-WRT, OpenWRT ja Tomato) tukemaan lisäprotokollia, esimerkiksi OpenVPN. VPN-palveluiden määrittäminen reitittimessä vaatii tietämystä verkon turvallisuudesta ja huolellista asennusta. Virheelliset konfiguroinnit VPN-yhteyksissä voivat jättää aukon ja samalla tehdä verkosta haavoittuvan.

6.6 VPN-protokollan edut ja haitat

VPN-protokollan suurimmat edut tulevat sen vahvasta salauksesta ja luotettavuudesta. Yhteyden ottaminen on mahdollista ainoastaan koneelta, joka on määritelty VPN-palomuurin konfigurointitietoihin. Tällaisia voivat olla esimerkiksi henkilökohtainen kannettava tietokone tai kotitietokone, sekä myös reitittimet on mahdollista konfiguroida. VPN-yhteyttä käytettäessä, yhteyden ollessa auki kaikki liikenne on vahvasti salattua, mutta kaikki tietokoneella oleva tieto on vapaasti luettavissa. Tästä syystä etäyhteyttä avattaessa ja käytettäessä on syytä huomioida ympäristöänsä ja pitää hyvää huolta teknisistä laitteistoista.

6.7 Palomuuri

Palomuurijärjestelmät ovat toteutettavissa joko laitteistolla tai ohjelmistolla, jonka tehtävänä on suojata sisäistä verkkoa ulkoverkosta saapuvilta hyökkäyksiltä. Palomuuri suo-

jaa vain ja ainoastaan sisäistä verkkoa, mikäli kaikki sisäinen ja ulkoinen verkkoliikenne kulkee sen lävitse. Palomuurin läpi pääsee ainoastaan rajatun tyyppinen liikenne. Mikäli palomuuri ei ole immuuni verkkohyökkäyksille, liikenne ei ole turvattua. Jos etäkäyttäjiä verkon ulkopuolelta sallitaan, tulee palomuurin ohjelmiston tukea VPN-yhteyspalvelua.

6.8 VPN ja palomuurit

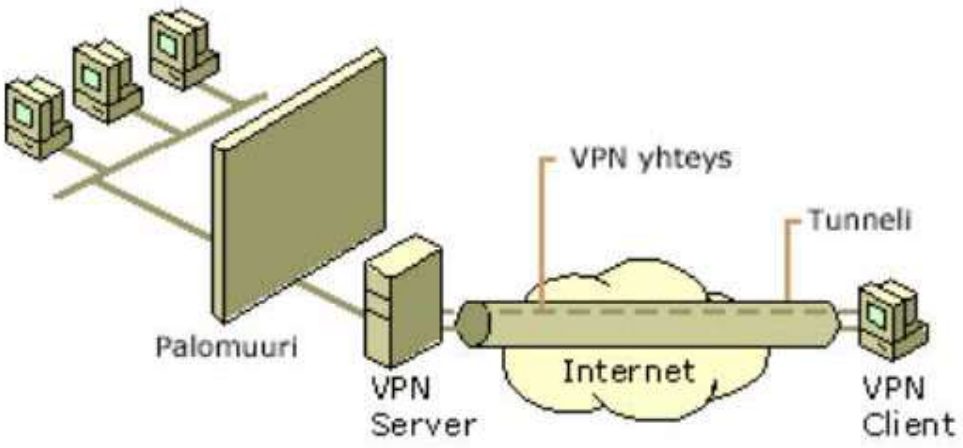
On kaksi lähtökohtaa käyttää palomuuria yhdessä VPN-palvelimen kanssa.

1 VPN-palvelin on yhteydessä internetiin ja palomuuri on VPN-palvelimen ja intranetin välissä.

2 Palomuuri on yhteydessä internetiin ja VPN-palvelin sijaitsee palomuurin ja intranetin välissä.

6.8.1 VPN-palvelin palomuurin edessä

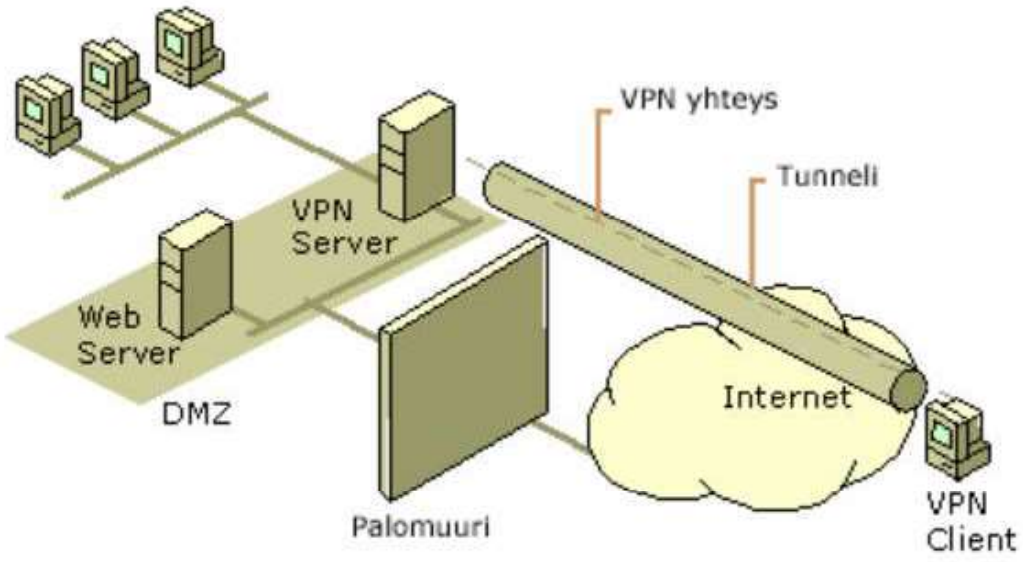
VPN-palvelimen ollessa kytkettynä internetiin palomuurin edessä, täytyy yhteydessä käyttää paketin suodattimia, jotka sallivat vain VPN-liikenteen edestakaisin VPN-palvelimen liittymän IP-osoitteista internetiin. Kun tunneloitu data on sisääntulevassa liikenteessä purettu VPN-palvelimella, se lähetetään eteenpäin palomuurille. Palomuuri hyödyntää suotimiaan liikenteen uudelleenohjauksen intranetin resursseihin. Koska ainoa liikenne, joka kulkee VPN-palvelimen kautta, on lähtöisin tunnistetuista VPN-clienteistä, palomuurin suodatusta käytetään tässä skenaariossa estämään VPN:n käyttäjiä hyödyntämästä tiettyjä Intranetin resursseja. Koska kaiken sallitun internetliikenteen on mentävä tässä tapauksessa VPN-palvelimen lävitse, tämä estää myöskin FTP:n ja Intranetin resurssien jakamisen VPN-verkkoon kuulumattomien käyttäjien kanssa. Kuviossa 11 esimerkki, kun VPN-palvelin on kytkettynä internetiin palomuurin edessä [13].



Kuvio 11. VPN-palvelin kytkettynä internetiin palomuurin edessä [13].

6.8.2 VPN-palvelin palomuurin takana

Useammin käytetty ratkaisu on kytkeä palomuuri internetiin ja VPN-palvelin muiden intranetresurssien kanssa demilitarisoidulle vyöhykkeelle (DMZ). DMZ on IP-verkon segmentti, joka yleensä sisältää resursseja internetkäyttäjille kuten web- ja FTP-palvelimia. VPN-palvelimella on liittymä sekä DMZ:ään että intranetiin. Tässä lähestymistavassa palomuuri täytyy olla konfiguroitu sekä syöte- että tulostussuodattimin. Koska palomuurilla ei ole salasana-avaimia kuten VPN-yhteydessä, se voi suodattaa ainoastaan selkokielisiä tunnisteita tunneloidussa datassa. Tämä ei kuitenkaan ole turvallisuusongelma, koska VPN-yhteys vaatii tunnistusprosessin, joka estää asiattomien pääsyn VPN-palvelimen toiselle puolelle. Palomuurin asetukset voidaan säätää siinä itsessään. Kuviossa 12 esimerkki, kun palomuuri on kytkettynä internetiin ja VPN-palvelin DMZ:aan [13].



Kuvio 12. Palomuuri kytkettynä internetiin ja VPN-palvelin DMZ:aan [13].

6.9 VPN-verkon ylläpito

Virtuaalista yksityisverkkoa täytyy ylläpitää aivan samoin kuin lähes kaikkia verkkoja. VPN:n turvallisuusasioissa, etenkin internet-yhteyksissä täytyy olla erittäin huolellinen. Seuraavia kysymyksiä kannattaa miettiä:

- minne käyttäjätiedot varastoidaan
- kuinka määritellään VPN-asiakkaiden osoitteet
- kuka saa luoda VPN-yhteyden
- kuinka VPN-palvelin tunnistaa yhteyttä yrittävän käyttäjän
- kuinka VPN-palvelin seuraa tapahtumia/pitää lokia
- kuinka VPN-palvelinta voidaan ylläpitää käyttäen normaaleja verkonhallintaprotokollia ja infrastruktuuria.

6.10 Käyttäjienhallinta

On hallinnollisesti epäkäytännöllistä luoda erillisiä käyttäjätilejä erillisille palvelimille samalle käyttäjälle ja yrittää pitää niitä ajan tasalla. Siksi tyypillisin käytäntö pääkäyttäjillä on luoda ”master”-käyttäjätietokanta esimerkiksi PDC- tai RADIUS-palvelimeen, joka sallii VPN-palvelimen hakea vahvistuksen yhdestä lähteestä. Käytön hallinta VPN-etäyhteyksissä tehdään konfiguroimalla käyttäjätilien soittoasetuksia. VPN-palvelimella pitää olla IP-osoitteita, jotta se pystyy paikantamaan ne VPN-palvelimen virtuaalisessa liittymässä ja VPN-asiakkaille (Client) osoitetut IP-osoitteet hankitaan DHCP:n kautta oletusarvoisesti.

7 Tietoturvallisen etäyhteyden toteuttaminen MB Connect Line-järjestelmällä

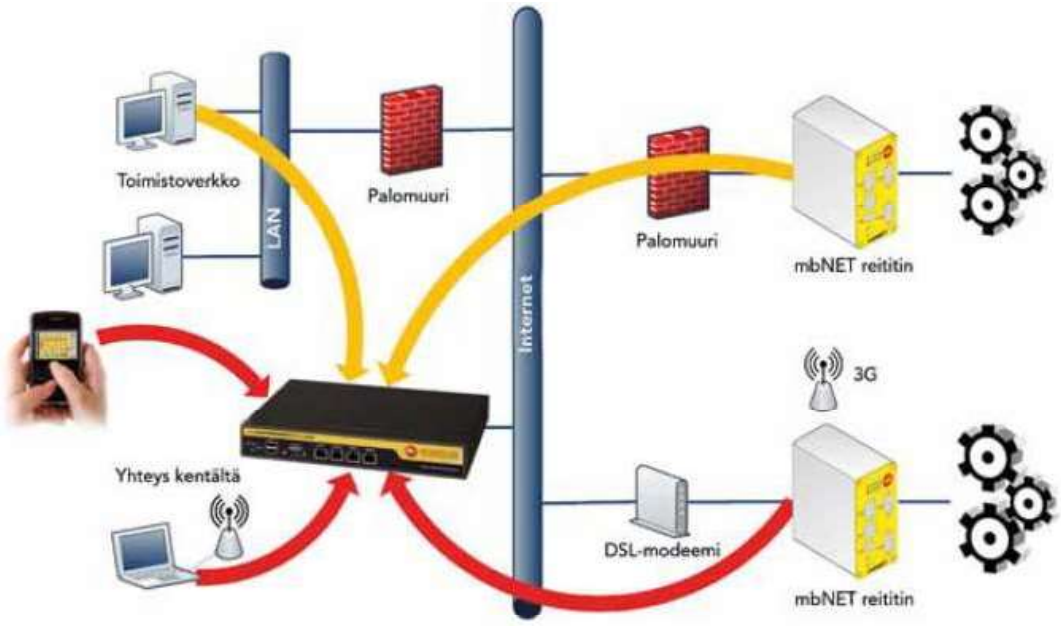
MB CONNECT LINE tarjoaa helposti hallittavan ja tietoturvallisen VPN-yhteyden sekä ethernet- että sarjaliikenteellä varustettuihin laitteisiin, mukaan lukien Siemens MPI ja Profibus DP. MbNET-laite asennetaan suoraan DIN-kiskoon ja se on rakenteeltaan teollisuuskäyttöön tarkoitettu.

Yhteys käyttäjän ja etälaitteen välille muodostetaan joko käyttämällä mbCONNECT24-pilvipalvelua tai fyysistä mymbCONNECT24-palvelinta, jossa käyttäjä aktivoi yhteyden haluttuun kohteeseen. Etäkohteen päästä yhteys muodostetaan joko internetverkon yli tai sisäänrakennetulla 3G-modeemilla (uusin malli 4G). MbNET-reitittimessä on paikka kahdelle SIM-kortille sekä lisäominaisuutena automaattinen varayhteyden käyttöönotto, joka mahdollistaa yhteyden muodostamisen, vaikka ensisijainen yhteys ei toimisikaan.

Ethernet-laitteet voidaan liittää reitittimen 4-porttiseen LAN-kytkimeen. MBNET osaa hoitaa liikenteen ohjauksen, joten liitetyn laitteen gateway-asetuksiin ei tarvitse tehdä ylimääräisiä konfigurointiasetuksia. Kaikki mbNET-laitteet konfiguroidaan joko pilvipalvelimella (tai omalla palvelimella), josta konfiguraatio siirretään mbNET-reitittimeen esim. USB-tikun avulla.

Etäohjelmointiyhteyttä varten PC tarvitsee valmistajan tarjoaman maksuttoman VPN-client-ohjelmiston. Koneen monitorointi on mahdollista MbWEB2go:lla myös ilman oh-

jelmistoasennuksia [14]. Kuviossa 13 on esitetty etäyhteysjärjestelmän toteutus kokonaisuudessaan.



Kuvio 13. Etäyhteysjärjestelmän toteutus [15].

7.1 MbNET-reitittimen ominaisuuksia

Reitittimen rakenne on suunniteltu teollisuuskäyttöön ja asennus onnistuu suoraan DIN-kiskoon. Etäyhteyteen voi käyttää joko WAN-liitäntää tai sisäänrakennettua 3G-modeemia (uusin malli myös 4G). Lisäksi reitittimessä on fyysiset liitännät ethernet- ja sarjaliikennelaitteille sekä Siemens MPI/Profibus DP sekä USB. Digitaaliset tulot ja lähdöt ovat konfiguroitavissa esim. etäyhteyden sallimiseksi ja aktiivisen yhteyden ilmaisuun. Reititin on liitettävissä myös jo olemassa olevaan VPN-palvelimeen [14].

7.2 MbNET-reititin

Reititin on varusteltu useilla eri tietoturvaprotokollilla, seuraavassa lueteltu protokollat tarkemmin:

- tuetut VPN-protokollat (IPSec, PPTP, L2TP, OpenVPN)
- sisäiset palomuurit: IP-suodatus Port Forwarding
- salaustavat: Blowfish, AES, DES / 3DES
- salausalgoritmit: MD5, SHA1
- autorisointi: PSK, X.509.

Kuviossa 14 on esitelty MbNET- reititin sarjaliikenteellä.

Kuvio 14. MbNET-reititin sarjaliikenteellä ja MPI/ProfiBus liitännällä [15].

7.3 MymbCONNECT24.virtual

MymbCONNECT24.virtual on monipuolinen etäyhteysalusta, jota voidaan hyödyntää sekä huoltoyhteyksissä että jatkuvan tiedonsiirron sovelluksissa, ja jonka ominaisuus on helppokäyttöisyys samoin kuin valmistajan pilvipalvelussa. Sillä voidaan toteuttaa laitevalmistajan etäpääsy laitteeseen tai tietoturvallinen VPN-verkko keskusvalvomon ja hajautettujen ala-asemien välille. Keskitetyn järjestelmän ansiosta reitittimien etähallinta ja ohjelmistopäivitykset sekä käyttäjien pääsynhallinta voidaan hallinnoida yhdestä paikasta. Järjestelmää voidaan hyödyntää myös hälytyspalvelimena ja kriittisissä sovelluksissa se voidaan kahdentaa. MymbConnect24- järjestelmällä voidaan toteuttaa varmatoiminen, täysin omassa hallinnassa oleva kokonaisuus, jota on helppo laajentaa uusien kohteiden mukaan. Koneenrakentaja voi mymbConnect24:n avulla tarjota asi-

akkailleen korkean palvelutason sekä tuottaa asiakkailleen tietoa toimitettujen koneiden toiminnasta. Jokaisen yhteyden toiminnasta voi kerätä tietoa ja seurata niitä palvelimen avulla.

Tietoturva on järjestelmän helppokäyttöisyydestä huolimatta erittäin korkealla tasolla, ja se tukee kaksivaiheista käyttäjien tunnistautumista (SMS, email, google authenticator). Tämän lisäksi palvelimessa on LDAP-liityntä kirjautumisoikeuksien tarkistamiseen esimerkiksi MS Active Directorystä.

Kentälle asennettava mbNET-etäyhteysreititin määritellään virtuaalipalvelimelle ja valmis konfiguraatio siirretään esimerkiksi USB-tikulla reitittimeen. Konfiguraation lataamisen jälkeen mbNET-reititin on välittömästi valmis käytettäväksi, eikä tietoturvallisen etäyhteyden luontiin mene kuin hetki aikaa.

VPN-palvelimella käyttäjälle asetetaan käyttäjäryhmä, joka määrittää sekä käyttäjän oikeudet palvelimella tehtäviin muutoksiin, että kohteet, joihin käyttäjällä on mahdollisuus muodostaa etäyhteys. Koneenrakentaja voi hyödyntää tätä ominaisuutta esimerkiksi tarjoamalla omille asiakkailleen kätevän ja tietoturvallisen etäyhteyden, jossa asiakas näkee ainoastaan omat laitteensa.

Virtuaali-VPN-palvelinta voidaan hyödyntää etäohjelmoinnin lisäksi myös jatkuvaan tiedonkeruuseen. Palvelimessa on fyysinen VPN-portti, jonka kautta tiedonkeruujärjestelmä voi olla jatkuvassa yhteydessä suoraan etäkohteisiin ilman, että se vaikuttaa ohjelmointiyhteyden muodostamiseen tai muuhun käyttöön. Etäyhteyksiin käytetään OpenVPN-protokollaa. OpenVPN tunnistaa järjestelmään yhteyttä ottavien koneiden ja käyttäjien oikeellisuuden sertifikaattien vaihdolla.

Järjestelmässä on valmiit työkalut etätiedonkeruun toteuttamiseen, ja valmiit liitäntäajurit ovat tarjolla esimerkiksi Siemens-, Modbus TCP- ja RTU- sekä Allen & Bradley-järjestelmiin, jolloin tieto kerätään ja puskuroidaan etäkohteessa ja synkronoidaan palvelimelle määräajoin. Kerättyä dataa voidaan esittää graafisesti palvelimella sekä siirtää tallennettavaksi ulkoiseen tietokantaan. Järjestelmää voidaan myös hyödyntää tietoturvalliseen tiedonsiirtoon etäkohteesta keskuspalvelimelle. Etäyhteyspalvelin ei käytä pilvitallennusta tai välityspalvelinta, vaan tieto siirtyy vain etäkohteen ja asiakkaan oman palvelimen välillä. MymbConnect24.virtual asennetaan VM-Ware vSphere-

virtuaaliympäristöön ja on laajennettavissa joustavasti 20000 etäyhteyteen asti. Kuvi-ossa 15 on esitetty yleinen esimerkki virtuaalisesta palvelinympäristöstä [14].

Kuvio 15. MymbCONNECT24 virtual-palvelinympäristö [15].

Taulukossa 3 on esitetty eri tyyppiset virtuaalipalvelimet sekä niiden ominaisuuksia

Taulukko 3. Virtuaalipalvelimia on kolme eri tyyppiä.

Ominaisuudet	**FREE**	**Factory Edition**	**Pro Corporate**
Etäjärjestelmätilien maksimi määrä	1	1	5
Reitittimiä maksimissaan	5	100	20000
Aktiivisia etäyhteyksiä maksi-missaan	1	250	250
M2M-ryhmien määrä	1	500	500

8 Dataliikenne mobiiliverkossa

Dataliikenne mobiili- / GSM-verkossa on ollut mahdollista siitä lähtien, kun verkko otettiin käyttöön. GSM:lle on Suomessa varattu taajuusalueet 880—915 MHz ja 925—960 MHz, jota kutsutaan GSM 900:ksi, sekä 1710—1785 MHz ja 1805–1880 MHz, tätä nimitetään GSM1800:ksi. GSM-verkko perustettiin aluksi pelkästään puhelinverkkona puheen siirtämistä varten, mutta dataliikenteen suuri kasvu on pakottanut verkkojen tiedonsiirtonopeuksien kehitykseen ja kasvattamiseen. Aluksi nopeudet olivat digitaalisessa 2G GSM-verkossa noin 9,6 ja 14,4 kbit/s, minkä jälkeen kehitettiin nopeampi GPRS. 3G tarjosi parannuksen nopeuteen ja varmuuteen UMTS- ja HSDPA-teknologioilla. Tällä hetkellä käytössä on 4G LTE (Taulukko 4.). 5G on suurten verkkolaitevalmistajien kuten Nokia, Ericsson, Huawei ja ZTE jatkuvissa keskusteluissa, koska edes osaltaan onnistuessaan se mullistaisi tämän hetken langattoman tiedonsiirtonopeuden.

Taulukko 4. Mobiiliverkon tiedonsiirtonopeuden kehitys [16].

Sukupolvi	**Tekniikka**	**Nopeus**
2G	GSM	14,4 kbit/s
2G	GPRS	40 kbit/s (teoriassa max.114 kbit/s)
2G	EDGE	200 kbit/s (teoriassa max.474 kbit/s)
3G	UMTS	10 Mbit/s (teoriassa max.21 Mbit/s)
3G	HSDPA	42 Mbit/s
4G	LTE	47 Mbit/s (teoriassa max.150 Mbit/s)

8.1 LTE-verkko

LTE (Long-Term Evolution), vapaasti suomennettuna ”pitkäaikainen kehitys”, on standardi nopeille langattomille mobiililaitteille ja datayhteyksille, jotka perustuvat GSM/EDGE- ja UMTS/HSPA-tekniikoihin. LTE lisää kapasiteettia ja nopeutta käyttäen erilaista radioyhteyttä sekä sisältää ydinverkkojen parannuksia. Standardin on kehittä-

nyt 3GPP (3rd Generation Partnership Project), ja se on määritelty Release 8-dokumenttisarjassa pienillä parannuksilla kuvattuna julkaisussa 9. LTE on päivitetty versio operaattoreille, joilla on tarjolla GSM/UMTS- sekä CDMA2000-verkko. LTE-taajuudet ja kaistat vaihtelevat eri maittain, ja siksi ainoastaan monikaista-versiota tukevat tuotteet pystyvät käyttämään LTE:tä maissa, joissa sitä tuetaan [16].

Yleisesti LTE:tä pidetään 4G-sukupolvena, mutta se ei täysin vastaa 4G teknologian teknisiä kriteerejä, jotka on kuvattu 3GPP:n Release 8 ja 9-dokumenttien vaatimusmäärityksissä. Tästä käytiin paljon keskusteluita ja lopulta todettiin, että LTE:tä yhdistettynä WiMAX- ja EHSPA 3G-teknologiaan voidaan kutsua 4G-sukupolven verkkotekniikaksi. [16]

> ”LTE on ensimmäinen 3G-tekniikka, jossa radioliikenteen suunta tukiasemasta päätelaitteeseen on toteutettu erilaisella radiotekniikalla kuin pääteasemasta tukiasemaan. Datan siirto tukiasemasta päätelaitteeseen tapahtuu OFDM-tekniikalla ja päätelaitteesta tukiasemaan SC-FDMA-tekniikalla. Data kulkee tukiasemasta päätelaitteeseen useita radioteitä pitkin eli niin sanotulla MIMO-tekniikalla, joka radiokanavan olosuhteista riippuen joko parantaa tiedonsiirron luotettavuutta tai mahdollistaa paljon tavallista suuremmat tiedonsiirtonopeudet. Standardi tukee monta erilaista tapaa MIMO:n hyödyntämiseen, joista paras valitaan tukiaseman ja päätelaitteen välillä valitsevien kanavaolosuhteiden mukaisesti. Mahdollisia ovat mm. perustekniikkana käytetty luotettavuutta parantava tila-taajuus-koodaus, tai olosuhteiden salliessa nopeuksia kasvattavat suljetun tai avoimen silmukan avaruudellinen limitys, tai lähetyksen tehoa suuntaava säteenmuodostus. Lisäksi voidaan käyttää solun kokonaiskapasiteettia kasvattavaa MU-MIMOa, jossa samaa aika-taajuus-resurssia käyttää monta eri käyttäjää.” [17].

Päätelaitteen ja tukiaseman etäisyyden ollessa 75 km MIMO-tekniikalla on kenttäkokeissa saatu dataa siirtymään tukiasemasta päätelaitteeseen 100 Mb/s ja päätelaitteesta tukiasemaan yli 50 Mb/s.

LTE on yhteensopiva nykyisen 3G-sukupolven verkkojen kanssa, ja sillä päästään nopeampiin ja luotettavampiin yhteyksiin, mihin sen tulevaisuuden menestys perustuu. Nokia ja Ericsson pääsivät demoissansa noin 150 Mb/s tiedonsiirtonopeuteen, mihin kaupallisten sovelluksien datansiirtonopeudet eivät yllä vielä pitkään aikaan, mutta silti 4G:n datansiirto on huomattavasti 3G-tekniikoita nopeampaa. Verkon arkkitehtuuri on LTE:ssä yksinkertaisempi, mikä lyhentää viiveitä tiedonsiirrossa ja vähentää operaattoreiden kustannuksia. Suurikokoiset solut (jopa yli 100 km) ovat myös mahdollisia, sekä tiedonsiirto nopeassa liikkeessä (jopa 350 km/h), mitä voidaan pitää LTE:n etuina. Lisäksi käyttöönottoa helpottaa sen joustavuus, koska standardi tukee useita taajuusalu-

eita, kaistanleveyksiä (1,4 MHz - 20MHz). LTE-tekniikan kehitys jatkuu tulevaisuudessa, vaikka 5G-sukupolven teknologiasta käydään suurta hypetystä [17].

8.2 5G-verkko

Entistä tehokkaampi 5G-verkko on tällä hetkellä kehityksen alla ja kaupallisessa käytössä arvioiden mukaan noin parin vuoden sisällä. 5G-verkko ei ole vain 4G-verkon parannus, vaan kokonaan uusi verkko, jossa yhteydet toimivat huomattavasti nopeammin kuin aikaisemmassa verkkoteknologiassa. 5G tuo myös lisää varmuutta verkkojen toimintaan ja parantaa erilaisten laitteiden välistä saumatonta ja reaaliaikaista kommunikointia. 5G ottaa käyttöön uusia taajuusalueita, koska 4G verkon taajuudet alkavat ruuhkautumaan. 5G:lle on määritelty kolme erilaista taajuusluokkaa eri käyttötarkoituksia varten. Alle 1 GHz:n taajuudet määritellään mobiiliverkkopalveluille ja IOT-laitteille. Laajennettuun mobiiliverkkoon on varattu 1—6 GHz:n taajuudet ja erittäin suurta tiedonsiirtonopeutta tarvitseville sovelluksille varataan yli 24 GHz:n taajuudet. Nämä niin sanotut millimetritaajuudet (>24 GHz) eivät läpäise seiniä [18].

9 Yhteenveto

VPN:ää pidetään edelleen erittäin tietoturvallisena ratkaisuna. VPN-yhteydessä hyvä ja luotettava tietoturva muodostuu itse VPN-yhteydestä, sekä joissain tapauksissa tunnelin sisällä ajettavasta salatusta yhteydestä, kuten SSH-menetelmää käyttämällä. Näin ollen menetelmä tarjoaa kaksinkertaisen suojauksen, joka on erityisen hyödyllinen esimerkiksi ylläpitotöitä tehtäessä ilman, että arkaluontoisia salasanoja, tunnuksia tai konfigurointitietoja pääsee vieraiden käsiin. SSL/TLS-protokollalla toteutettu ratkaisu ei ole aivan yhtä joustava, turvallinen ja helposti toteutettavissa kuin VPN-menetelmä. VPN-yhteyden käyttö on helppoa, koska siinä tarvitsee vain avata tunneli VPN-asiakkaalle kertomalla käyttäjätunnus ja salasana, minkä jälkeen kaikki lähetettävä ja vastaanotettava data on suojattu ulkopuolisilta.

Kun toimenpiteet on hoidettu oikein, ei kummassakaan yhteysmuodossa juurikaan ole huonoja puolia. Ainoat huonot puolet kohdistuvat lähinnä pääkäyttäjälle lisätyönä uusien työasemien konfigurointina.

Insinöörityössä tavoite oli tutkia tiedonsiirron salaavia protokollia ja turvallisuustekniikoita estämään verkkohyökkäyksiä. Työn tekeminen on tarjonnut valtavasti uutta tietoutta etäyhteyksistä, tieto- ja kyberturvasta sekä IOT:stä. Runsaasti uutta tietoa on saatu myös VPN:stä, SSL/TLS:stä ja näiden salaustekniikoista.

Lähteet

1 Mazhelis, Oleksiy & Warma, Henna. 2013. Internet-of-Things Market, Value Networks, and Business Models: State of Art Report. s.9-10.

2 IOT and M2M, what is the difference? Verkkoaineisto. https://www.incognito.com/blog/iot-and-m2m-whats-the-difference/ [Luettu 14.5.2018.]

3 Viestintävirasto. Verkkoaineisto. https://fi.wikipedia.org/wiki/Viestint%C3%A4virasto. [Luettu 23.4.2018.]

4 What is SSL, TLS and HTTPS? Verkkoaineisto. https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https [Luettu 3.5.2018.]

5 Kyberturvallisuus. Verkkoaineisto. https://fi.wikipedia.org/wiki/Kyberturvallisuus [Luettu 5.5.2018.]

6 Rousku Kimmo. Kyberturvallisuus – mitä se oikeastaan on? Verkkoaineisto. https://www.tivi.fi/blogit/2012-09-06/Kyberturvallisuus---mit%C3%A4-se-oikeastaan-on-3194338.html [Luettu 5.5.2018.]

7 Kerttula, Esa. 1998. Tietoverkkojen tietoturva. Oy Edita Ab, Helsinki

8 Kryptologia. Verkkoaineisto. https://fi.wikipedia.org/wiki/Kryptologia [Luettu 8.5.2018.]

9 PKI. Verkkoaineisto. https://en.wikipedia.org/wiki/Public_key_infrastructure [Luettu 19.5.2018.]

10 TLS. Verkkoaineisto. https://en.wikipedia.org/wiki/Transport_Layer_Security [Luettu 19.5.2018.]

11 Virtual Private Network. Verkkoaineisto. https://en.wikipedia.org/wiki/Virtual_private_network [Luettu 20.5.2018.]

12 VPN-Virtual Private Network. TKK, tietoverkkolaboratorio. Verkkoaineisto. https://www.netlab.tkk.fi/opetus/s38118/s98/htyo/27/vpn.shtml. [Luettu 20.5.2018.]

13 VPN-verkot. Verkkoaineisto. https://www.2kmediat.com/vpn/palomuurit.asp [Luettu 30.5.2018.]

14 MB Connect Line. News. Verkkoaineisto. https://www.mbconnectline.com/en/news/product-news.html. [Luettu 21.5.2018.]

15 MB Connect Line. Product overview. Verkkoaineisto. https://www.mbconnectline.com/en/products/product-overview.html. [Luettu 23.5.2018.]

16 LTE. Verkkoaineisto. https://en.wikipedia.org/wiki/LTE_(telecommunication). [Luettu 27.5.2018.]

17 LTE. Verkkoaineisto. https://fi.wikipedia.org/wiki/LTE. [Luettu 21.5.2018.]

18 5G. Verkkoaineisto. https://en.wikipedia.org/wiki/5G. [Luettu 22.5.2018.]