YRITYSTEN ETÄKÄYTTÖ-OHJELMISTOJEN TIETOTURVA

LAHDEN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma
Yritysviestintäjärjestelmät
Opinnäytetyö
Kevät 2006
Vesa Piispanen

Lahden Ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

PIISPANEN, VESA: Yritysten etäkäyttöohjelmistojen tietoturva

Yritysviestintäjärjestelmien opinnäytetyö, 44 sivua, 0 liitesivua

Kevät 2006

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on selvittää, miten tietoturvallisuus on toteutettu etäkäyttöohjelmistoissa. Tutkin opinnäytetyössäni esiintyviä etäkäyttöohjelmia käyttäjän näkökulmasta. Selvitän miten etäkäyttöohjelmistot hyödyntävät käyttäjähallintoa ja minkälaisten tietoliikenneyhteyksien avulla on mahdollistaa suorittaa etätyötä. Etätyöskentely on työntekijöiden keskuudessa kerännyt suosiotaan, joten käsittelen myös yleisellä tasolla etätyötä.

Opinnäytetyöni alkuosiossa selvitän kirjallisuutta ja Internetiä hyväksi käyttämällä erilaisten salaus-, VPN- ja käyttäjäntunnistusmenetelmien toimintaa ja ratkaisuja. Teoriaosion jälkeen selvitän miten niitä on hyödynnetty erilaisissa etäkäyttöohjelmistoissa, jotta tietoturvallinen etätyö olisi mahdollista.

Käyn työssäni läpi kolmen etäkäyttöohjelmiston tietoturvan toteutuksen: Symantec PcAnywheren, Laplink Gold:n ja Citrix Metaframen. Nämä etäkäyttöohjelmistot sisältävät joukon erilaisia tietoturvaominaisuuksia, joiden avulla on mahdollista suorittaa etätyötä tietoturvallisesti riippumatta käytettävästä tietoliikenneyhteydestä tai etäyhteyteen käytettävästä etätyöasemasta. Symantec PcAnywhere ja Laplink Gold ovat puhtaasti etäkäyttöön soveltuvia ohjelmistoja, kun taas Citrix:n ratkaisu tarjoaa ohjelmistot etäkäyttöön etätyöasemille.

Etätyön merkitys mobilisoituvassa yhteiskunnassa on kasvamassa, joten on tärkeää valita oikeanlainen etätyöratkaisu, helpottaakseen ja varmistaakseen riittävä tietoturva käyttäjien keskuudessa.

Avainsanat: etäkäyttö, etätyö, VPN, tietoturvallisuus

Lahti University of Applied Sciences
Faculty of Business Studies
Degree Program in Computing

PIISPANEN, VESA: Corporations' remote control software's information security

Bachelor's Thesis of Business Information Systems, 44 pages, 0 appendices

Spring 2006

ABSTRACT

This thesis deals with how remote control software's information security is carried out. In this thesis I study remote control software from the user´s point of view and how remote control software programs utilize user administration, and what kind of communication links are used to allow remote work. Telecommuting has increased popularity among workers. Consequently, remote work at a general level is also discussed.

The first part of the thesis deals with literature and different encryption-, VPN- and user authentication methods and solutions are explored with the help of the Internet. After theory section, I explain how these methods have been used in different remote control software so that the remote work would be secured and possible.

I audit the information security implementation of three remote control software programs: Symantec PcAnywhere, Laplink Gold and Citrix Metaframe. These remote control software programs include different kinds of information security details which make it possible to do remote work securely regardless of the communication connections used or the remote workstation. Symantec PcAnywhere and Laplink Gold are used in remote work exclusively, whereas the Citrix solution offers software to remote workstations.

The importance of telecommuting in our mobile society is increasing. Therefore, it is important to choose the correct remote work solution, to ease and secure sufficient information security among workers.

Key words: remote use, remote work, VPN, data security

SISÄLLYS

1 JOHDANTO

Nykypäivänä erilaiset yritykset ja organisaatiot ovat oppineet hyödyntämään tietotekniikan luomia mahdollisuuksia niin liiketoiminnassa kuin työntekijöidenkin apuna. Tietotekniikan päätehtävänä onkin tukea yrityksen liiketoimintaa. Erilaisten tietoliikenneyhteyksien ja tietojärjestelmien hankinta sekä suunnittelu, vaatiikin yrityksien päättäjiltä harkittuja päätöksiä, jotta saavutettaisiin asetetut tavoitteet.

Käyn opinnäytetyössäni läpi esiintyviä etäkäyttöohjelmia käyttäjän näkökulmasta. Selvitän miten etäkäyttöohjelmistot hyödyntävät käyttäjähallintoa, ja lisäksi tutkin etäkäyttöohjelmistojen tietoliikenneyhteyksiä ja tietoturvaa. Etätyöskentely on työntekijöiden keskuudessa kerännyt suosiotaan, joten käsittelen myös yleisellä tasolla etätyötä.

Tutkin opinnäytetyössäni tarkemmin VPN-yhteyttä, joka mahdollistaa etätyöntekijälle tietoturvallisen yhteyden. Opinnäytetyöni keskittyy yrityksien etäkäyttöohjelmistojen pariin, joista tuon esille Symantec PcAnywhere:n, Laplink Gold:n ja Citrix Metaframe Presentation Server:n. Kaksi ensimmäistä ohjelmistoa ovat pääasiassa kahden työaseman välisiä etäkäyttöohjelmistoja, joiden avulla voidaan ottaa yhteyttä, niin toiseen työasemaan kuin palvelimeenkin. Citrix Metaframe perustuu keskitettyyn ohjelmistojen jakamiseen ja hallinointiin palvelimilta käsin. Citrix Metaframe:n tarjoaman ICA-asiakasohjelmiston avulla muodostetaan VPN-yhteys Metaframe palvelimeen kotoa tai yrityksen lähiverkosta käsin. Tämän avulla saadaan yrityksen tarjoamat sovellukset käyttöön joka paikassa. Citrix Metaframe mahdollistaa sovelluksien jakamisen niin yrityksen lähiverkkoon kuin myös etätyöntekijälle.

Suoritin tutkimukseni teoreettisena kirjoituspöytätutkimuksena eli hyödynsin tutkimuksessani jo valmiina olevaa tietomateriaalia, kirjallisuutta ja Internetiä. Opinnäytetyöni päätutkimusongelmat ovat:

- Miten etäkäyttöohjelmistojen tietoturva on toteutettu?

- Minkälaisia tietoliikenneyhteyksiä etätyöntekijän on mahdollista hyödyntää etäkäyttöohjelmien kanssa?
- Etäkäyttöohjelmistojen käyttökohteet?

2 ETÄTYÖ

Etätyö mahdollistaa työn tekemisen etänä oman aikataulun mukaisesti työnantajan ohjeita ja työmääräyksiä noudattaen. Etätyöskentely mahdollistaa myös työ- ja kotiaskareiden helpomman organisoimisen. Toisaalta etätyössä voidaan kokea haittana se että työ ja vapaa-aika eivät eroa ainakaan konkreettisesti toisistaan. Etätyöntekijä on oikeutettu samoihin etuuksiin, kuin muutkin työntekijät. (Etätyö kiinnostaa)

Etätyö kiinnostaa -artikkelin mukaan: ”Suomi on kansainvälisessä vertailussa etätyön edelläkävijöitä. Välimatkat maassamme ovat pitkiä, tietokoneet ja -verkot ovat lähes kaikkien ulottuvilla, koulutus on korkeatasoista ja työ on maantieteellisesti ja organisaatioiden ja henkilöstönkin näkökulmasta epätasaisesti jakautunut. Kuitenkin vain alle prosentti Akavan työmarkkinakyselyyn vastanneista oli tehnyt etätyötä kokoaikaisesti. Etätyön suurin este lienevät asenteet ja vanhat toimintamallit. Noin puolet akavalaisista arvioi, että ainakin osan tehtävistä voisi hoitaa kotoa käsin.”

Etätyöntekijän on hyvä solmia työnantajan kanssa ehdoista, joiden mukaan palkka määräytyy. Lisäksi mahdollisista etäyhteyden, työaseman ja oheislaitteiston kustannuksista on hyvä sopia etukäteen. (Etätyö kiinnostaa)

3 TIETOTURVA

3.1 Yleistä

Tietoturvalla pyritään parantamaan yrityksen työntekijöiden työntekoa paikasta ja kellonajasta riippumatta. Tietoturvan avulla pyritään myös jakamaan työntekijöille yrityksen verkkoresursseja ja muuta tietoa, jotta ne olisivat työntekijöiden käytössä. Tämä tarkoittaa myös sitä että tiedot ovat vain ja ainoastaan niiden henkilöiden käytössä, jotka yrityksen resursseja tarvitsevat. Tietoturva on jaettu viiteen tietoturvapalveluun: luottamuksellisuus, autentisuus, kiistämättömyys, eheys ja käytettävyys. (Ruohonen 2002, 2)

- Luottamuksellisuudella pyritään tietojärjestelmästä antamaan tietoja henkilöille, jotka ovat tietojen saamiseen oikeutettuja.
- Autentikoinnin avulla pystytään tunnistamaan kaikki tietojärjestelmän osat, esimerkiksi käyttäjän kirjautuminen yrityksen järjestelmään.
- Kiistämättömyys tarkoittaa tehdyn tapahtuman kirjaamista ja todistamista myöhemmässä vaiheessa.
- Eheyden tavoitteena on tietojärjestelmän tietojen eheys, eli tietojärjestelmässä olevat tiedot eivät pääse muuttumaan luvattoman tahon toimesta.
- Käytettävyys on tärkein palvelu, jonka tarkoituksena on varmistaa tietojärjestelmän toimivuus, jotta tietojärjestelmän tiedot ovat aina käytettävissä.

(Ruohonen 2002, 3)

3.2 Tietoturvan osa-alueet

Tietojärjestelmän osalta tietoturva voidaan jakaa seuraaviin osa-alueisiin: tietoaineisto-, ohjelmisto-, tietoliikenne-, fyysinen-, laitteisto-, henkilöstö-, käyttö- ja hallinnollinen turvallisuus (Ruohonen 2002, 4). Näillä jokaisella osa-alueella on oma merkityksensä ja tärkeytensä yrityksen tietoturvallisuudessa. Yrityksessä onkin tärkeää tunnistaa osa-alueet, jotka vaativat parannusta tai muutosta. Jokainen yrityksen työntekijä on ratkaisevassa asemassa yrityksen tietojärjestelmien tietoturvallisuudessa, sillä jos jollakin osa-alueella on puutoksia, voivat ulkopuoliset henkilöt päästä yrityksen tietojärjestelmiin käsiksi.

- Tietoaineistoturvallisuus koostuu tiedostojen suojaamisesta salasanoin, käyttöoikeuksien määrityksellä, varmuuskopioinnilla ja virusohjelmistojen avulla.
- Ohjelmistoturvallisuudella tarkoitetaan yrityksessä käytössä olevien ohjelmistojen lisensointia ja niiden ylläpitoa.
- Tietoliikenneturvallisuudella varmistetaan tietoliikenteen turvallisuus, jotta ulkopuoliset henkilöt eivät pääse lähetettävään tai vastaanotettavaan tietoon käsiksi. Eräs tällainen tietoturvallinen tietoliikenneratkaisu on VPN-yhteys.
- Fyysisellä turvallisuudella tarkoitetaan yrityksen tilojen suojaamista ulkopuolisilta uhkilta.
- Laitteistoturvallisuudella voidaan estää ulkopuolisten henkilöiden pääsemistä käsiksi yrityksen työasemiin, palvelimiin ja muuhun järjestelmään. Laitteistoturvallisuutta voidaan parantaa erilaisilla kulkuluvilla, henkilökorteilla ja työntekijöiden aktiivisella työympäritön tarkkailulla.
- Henkilöstöturvallisuutta voidaan kontrolloida tarkastamalla työntekijöiden taustat jo ennen työn alkamista ja antamalla käyttäjille riittävästi koulutusta, jotta tahattomilta virheiltä vältyttäisiin.
- Käyttöturvallisuus on osa henkilöstöturvallisuutta ja sillä pyritään tietojärjestelmien turvalliseen käyttöön.

- Hallinnollinen turvallisuus perustuu tietoturvallisuuden osa-alueiden johtamiseen hallitusti kehittämällä ja luomalla tietoturvaa.

(Ruohonen 2002, 4-5)

4 ETÄKÄYTTÖOHJELMISTOT

4.1 Yleistä

Etäkäyttöohjelmia käytetään etätyössä. Etäkäyttöohjelmille on ominaista, että ne lähettävät verkon välityksellä vain näppäimistö- ja hiirikomennot etäyhteyden toiseen päähän, tietokoneeseen (toinen työasema tai palvelin) johon yhteys ollaan luotu. Etäyhteyden avulla etäkäyttäjä voi käyttää hyväkseen palvelimen tai työaseman tarjoamia resursseja, kuten tulostus- ja tiedostojenhallinta mahdollisuuksia. Ohjelmien suoritus tapahtuu paikallisessa etäyhteyden päässä olevassa työasemassa ja vain kuvaruudulla näkyvä kuva siirretään verkon välityksellä etätyöasemalle. Tämä ratkaisumalli mahdollistaa raskaidenkin sovelluksien käytön nopeuksien kärsimättä. Joitakin etäkäyttösovelluksia voidaan käyttää myös mikrotukitehtävissä, jolloin niiden avulla voidaan mm. asentaa ohjelmia. (Paananen 2003, 233)

Lähiverkon etäkäyttö mahdollistaa tiedon hakemisen yrityksen lähiverkosta etäyhteydellä. Yleensä etäkäyttö perustuu käyttäjän tunnistamiseen salasanojen, puhelinnumeroiden tai tietyn VPN (Virtual Private Network) –ohjelman avulla. (Paananen 2003, 276-277)

Etäkäytöllä on mahdollista käyttää yrityksen tarjoamia ohjelmia yrityksen lähiverkosta tai hakea tarvittavaa dataa esim. tietokannoista. Etäkäyttö mahdollistaa myös verkon ylläpitäjille mahdollisuuden hallita lähiverkkoa ja

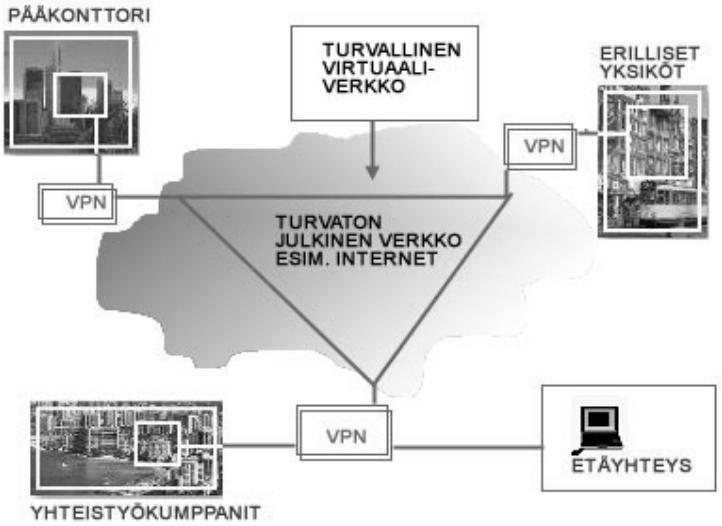
palvelimia, vaikka yrityksen ulkomaisesta toimipisteestä käsin. Etäkäyttö mahdollistaa siis myös kaukaisten verkkojen hallinnan. (Paananen 2003, 276-277)

Yrityksien lähiverkot yhdistetään toisiinsa teleoperaattorien ja lisäarvotuottajien tarjoamilla etäyhteyspalveluilla. Yhteyspalvelun valintaan vaikuttavat monet eri osa-alueet, kuten verkkojen etäisyys toisistaan, verkkoliikenteen määrä, verkkoliikenteen jakautuminen ajallisesti, sijaintimaa jne. Yrityksen miettiessä oikeanlaista ratkaisua verkkojen välisiin etäyhteyksiin, on tärkeää tunnistaa yrityksen tarpeet, jotta päästään haluttuun ratkaisuun. (Puska 2000, 222)

4.2 Virtuaaliset yksityisverkot

VPN (Virtual Private Network) eli virtuaalinen yksityisverkko, mahdollistaa yrityksen yksityisen tietoliikenneverkon sekä sisäisen tiedon jakamisen julkista verkkoa hyväksikäyttämällä. VPN-verkko toimii tunnelointi periaatteella, jolloin näitä tunneleita pitkin voidaan muodostaa salattu yhteys yrityksen pääkonttorin, etäkäyttäjän ja erillisten toimipisteiden välillä. (Hakala & Vainio 2002, 318)

Etätyöntekijän työaseman ja pääkonttorin välinen VPN-yhteys muodostetaan VPN-asiakkaana olevan työaseman ja etäkäyttöpalvelimen välille. VPN-yhteyden muodostamiseen käytetään yleensä VPN-asiakasohjelmaa (client), joka ottaa yhteyden VPN-palvelimeen tai VPN-palomuuriin. VPN-ohjelma tunneloi kaikki etäkäyttäjän lähettämät paketit salausprotokollan avulla ja muodostaa yhteyden yrityksen verkkoon. Toimipisteiden välinen VPN-yhteys voidaan muodostaa VPN-reitittimien välille. Reititin tarkkailee toimipisteestä ulospäin menevää liikennettä, kun reititin havaitsee ulospäin suuntautuvaa liikennettä, joka on menossa yrityksen toiseen toimipisteeseen, salaa se liikenteen kapseloimalla sen IP-paketin sisälle ja lähettää sen vastaanottavalle reitittimelle. Vastaanottava reititin purkaa IP-paketin sekä salauksen, ja reitittää sen eteenpäin oikealle koneelle. (Hakala & Vainio 2002, 318)



KUVIO 1. Havainnollistaa VPN-yhteyttä eri käyttäjien välillä. (VPN-verkot)

4.2.1 VPN-mallit

VPN-palveluja ja ratkaisuja on tarjolla lähes loputon määrä ja tarjottavista malleista on helppo löytää omiin tarpeisiin sopiva VPN-ratkaisu, jos tiedossa on yrityksen tarpeet tulevalle VPN-ratkaisulle. Käyn tutkielmassani läpi kolme yleisintä VPN-mallia.

4.2.1.1 Tarjoajamalli

Tarjoajamallissa VPN-yhteys on toteutettu lähes kokonaan palveluntarjoajan infrastruktuuriin, joten asiakas on riippuvainen palveluntarjoajasta. VPN-yhteyksien toiminta ja ylläpito kuuluu palveluntarjoajalle, joten asiakas ei voi vaikuttaa yhteyksien toimivuuteen. VPN-yhteyksien nopeudet ovat yleensä tarjoajamallissa hyvät, koska palveluntarjoajan resurssit ovat suuret ja laajentaminen myöhäisemmässä vaiheessa onnistuu helposti. VPN-tunnelointi suoritetaan palveluntarjoajan verkossa, joten se on kalliimpi ratkaisu verrattaessa sitä muihin VPN-malleihin. (Perlmutter & Zarkower 2001, 88-92)

4.2.1.2 Sekamalli

Sekamallille on hyvin tyypillistä, että VPN-tunnelin toinen pää on palveluntarjoajan verkossa ja toinen pää asiakkaan verkossa. Silloin palveluntarjoajalla on vastuu etäkäyttäjien VPN-yhteyksien aloittamisesta ja toimittamisesta asiakkaan verkkoon. Sekamalli ei sido asiakasta vain yhden palveluntarjoajan piiriin, vaan asiakkaalla on mahdollista käyttää myös muita palveluntarjoajia, koska tunneloinnin toinen pää sijaitsee aina asiakkaan omissa tiloissa. Toisaalta tunnelin sijoittuminen asiakkaan tiloihin saattaa johtaa ristiriitoihin VPN-verkon konfiguroinnissa. (Perlmutter & Zarkower 2001, 93-97)

4.2.1.3 Päästä-päähän –malli

Päästä-päähän –malli on yleisimmin toteutettu VPN-yhteys malli. Palveluntarjoajan rooli tässä mallissa on lähes olematon, sillä palveluntarjoaja toimii vain datan välittäjänä. Erilaiset etäkäyttö VPN-yhteydet ja toimipaikkojen väliset salatut yhteydet toteutetaan käyttämällä päästä-päähän –mallinnusta. Kyseistä VPN-mallia käyttävät yritykset vastaavat myös sen ylläpidosta, mutta palveluntarjoajilla voi olla palveluita, joiden avulla asiakkaan laitteistot integroidaan palveluntarjoajan toimesta. Etäkäyttö VPN:n asiakasohjelmistot (client) saattavat muodostaa mikrotuelle työtä ja päänvaivaa, sillä ohjelman käyttö ja sen jakelu etäyhteyttä haluaville voi olla hankalaa. Kuviossa 1 voisi olla hyvinkin käytössä päästä-päähän –malli. (Perlmutter & Zarkower 2001, 98-101)

4.2.2 VPN-tunnelointiprotokollat

VPN-tekniikka perustuu tunnelointiin. Tunnelointi salaa julkisessa verkossa liikkuvan datan, jotta ylimääräiset osapuolet eivät pääse siihen käsiksi.

Tunnelointi tarkoittaa pakettien kapselointia toisten pakettien sisään. Tunnelointi mahdollistaa seuraavia etuja:

- yksityisten osoitteiden piilottaminen
- muun kuin IP-protokollaa noudattavan datan kuljettaminen
- datan johtamisen helpottaminen
- sisäärakennetun turvallisuuden huolehtiminen

(Perlmutter & Zarkower 2001, 104-105)

4.2.2.1 IPSec

IPSec-protokolla tarjoaa IP-paketeille koskemattomuutta ja luottamuksellisuutta. Jotta IPSec pystyisi täyttämään em. ominaisuudet, sen täytyy koostua kolmesta perustekijästä: todennus (pakettitasolla), salaus ja avaimenhallinta.

- Todennuksen (authentication) avulla voidaan varmistaa lähetetyn datan lähettäjät, sekä lähetetyn datan sisällys. Pakettitason todennus hoidetaan IPSec-otsakkeen (Authentication Header) avulla.
- Salaus (encryption) toimenpide salaa datan niin, että se on käsittämätön niille, joiden hallussa ei ole oikeaa avainta. IPSec tukee myös datakuorman salausta ESP-protokollan (Encapsulating Security Protocol) avulla.
- Avaimenhallinta mahdollistaa neuvottelun salatusta avainarvosta lähettäjän ja vastaanottajan välillä.

(Perlmutter & Zarkower 2001, 106-107)

IPSec-protokolla toimii siten, että sen on ensimmäiseksi sovittava yhteisestä avaimesta lähettäjän ja vastaanottajan välillä. Se tapahtuu jonkin IPSecin tukeman menetelmän avulla, manuaalisesti, staattisella konfiguraatiolla tai dynaamisesti standardeja käyttämällä. Avainten neuvottelun jälkeen IPSecin on mahdollista muodostaa turvallisuusliitto lähettäjän ja vastaanottajan välille. Seuraavaksi datan lähettäjän on lisättävä lähetettävään dataan digitaalinen allekirjoitus avaimen arvoja käyttämällä. ESP-salausta käytettäessä on mahdollista salata myös itse liikkuva tieto. Suosituimpia IPSecin yhteydessä käytettäviä salausalgoritmeja ovat

DES (Data Encryption Standard, 64bit), 3DES (128bit) ja RC4. Kun allekirjoitus on lisätty dataan ja mahdolliset salaukset tehty, lähettäjä lähettää datan verkkoon kohti datan vastaanottajaa. (Perlmutter & Zarkower 2001, 109-110)

Toisessa päässä vastaanottaja saa paketin ja käyttää avainta purkaakseen paketin algoritmin, jotta data voitaisiin palauttaa alkuperäiseen muotoonsa. Tämän jälkeen paketti lähetetään verkossa eteenpäin kohti päämääräänsä. (Perlmutter & Zarkower 2001, 111)

Vastaanottajana voi olla VPN-sovellus tai -laite, joka on vastuussa IPSec-liittojen hoitamisesta. Vastaanottaja joutuu pitämään kirjastoa erilaisista avaimista ja algoritmeistä, sillä VPN-yhteyksiä voi olla monia yhdestä laitteesta. (Perlmutter & Zarkower 2001, 111)

4.2.2.2 PPTP

PPTP (Point-to-Point Tunneling Protocol) on Microsoftin kehittämä etäkäyttöprotokolla, joka tukee erilaisia verkkoprotokollia.VPN-tunnelin PPTP-muodostaa tunneloimalla PPP-kehykset TCP/IP-pohjaisen verkon kautta. PPTP on erittäin joustava tunnelointiprotokolla, sillä sitä voidaan käyttää soittoyhteyksissä, lähiverkoissa(LAN), laajan alueen verkoissa (WAN), TCP/IP-verkoissa ja Internetissä. (Perlmutter & Zarkower 2001, 115-116)

PPTP-tunneli aloitetaan muodostamalla yhteys TCP-istuntopalvelimen ja PPTP-asiakkaan välillä. Kun yhteys on muodostettu, voidaan lähettää PPTP-valvontaviestejä asiakkaan ja palvelimen välillä. Kun tunneli on toiminnassa, voidaan lähettää GRE-prokollalla (Generic Routin Protocol) kapseloituja datapaketteja palvelimen ja asiakkaan välillä. Kun asiakas lopettaa tunneloidun yhteyden, hän lähettää PPTP-valvontapaketin palvelimelle, joka lopettaa istunnon ja katkaisee tunnelin. (Perlmutter & Zarkower 2001, 116)

4.2.2.3 L2TP

L2TP (Layer 2 Tunneling Protocol) on Microsoftin ja Ciscon kehittelemä tunnelointiprotokolla. Se syntyi PPTP- ja L2F (Layer 2 Forwarding)-protokollien sulautumisen myötä. Tulevaisuudessa L2TP tulee syrjäyttämään Ciscon kehittelemän L2F:n. (L2TP)

L2TP-tunnelointiprotokollaa käytetään pääasiassa vain sekamallissa, jolloin L2TP-tunneli aloitetaan palveluntarjoajan verkossa ja päätetään asiakkaan verkkoon. LAC (L2TP Access Concentrator)-yhteyskeskitin ja LNS (L2TP Network Server)-verkkopalvelin ovat L2TP VPN-verkon keskeisimpiä komponentteja, joiden avulla VPN-yhteys muodostetaan. (Perlmutter & Zarkower 2001, 126-127)

LAC-yhteyskeskittimen tehtäviä ovat:

- Modeemi- ISDN-puheluiden päättäminen
- Ensimmäisen tason todennus ja tunnelointi käyttämällä Radiusta
- PPP:n alun käynnistäminen, jonka LNS kumoaa myöhemmin lähes kokonaan
- L2TP-protokollan suorittaminen komento- ja valvontaviestien avulla sekä kapselointi etäkäyttäjän PPP-liikenteen L2TP-portteihin

(Perlmutter & Zarkower 2001, 126-127)

LNS-verkkopalvelin toimii ohjelmistotoimintona asiakaspäässä ja sen tehtäviin kuuluu toimia PPP-avaintoimintojen suorittajana. Se voi lisäksi suorittaa myös valinnaisia toimintoja, kuten RADIUS:sta (todennus, autorisaatio ja tilinpito), suodatusta, Multilink-PPP:N päättämistä ja ulossoittoa. L2TP käyttää komento-, valvonta- ja datapaketteja, jotka ovat UDP-kapseloituja eli ns. yhteydettömiä. Vaikka L2TP-verkko on ns. yhteydetön, se suoriutuu paremmin korkeiden saantiviiveiden verkoissa. (Perlmutter & Zarkower 2001, 126-129)

4.2.2.4 SSH

SSH (Secure Shell) on suomalaisten kehittämä salausprotokolla ja sitä voidaan käyttää myös tunnelointiin. Se on tarkoitettu lähinnä pääte-yhteyksille, ja se toimii omana ohjelmana työasemassa ja palvelimessa. SSH-yhteys muodostetaan palvelinohjelmaan käynnistämällä työasemassa oleva SSH-asiakasohjelma. Tunneloidulla SSH-yhteydellä voidaan avata yhteyksiä, jotka muuten pysäytettäisiin palomuurissa. SSH-yhteys on salakirjoitettu, joten virustorjuntaohjelmistot eivät pysty analysoimaan tietoa. (Ruohonen 2002, 287)

SSH-yhteys jakaa toimintansa kolmeen eri kerrokseen: siirtokerrokseen, käyttäjäntunnistuskerrokseen ja yhteyskerrokseen.

SSH-yhteys avataan siirtoprotokollan avulla, ja se toimii TCP-protokollan päällä. Siirtokerros huolehtii työaseman ja palvelimen tunnistamisesta, viestien eheydestä ja niiden salakirjoittamisesta. Yhteyden luonnin alussa osapuolet sopivat mm. käytettävistä pakkaus- ja salakirjoitusmenetelmistä, istuntoavaimesta, palvelimen tunnistamisesta sekä eheyden varmistavasta hash-functiosta. Kun yhteys on muodostettu osapuolien välille, kaikki liikenne tapahtuu salakirjoitettuna. (Ruohonen 2002, 287-288)

Käyttäjäntunnistuskerroksen tehtävänä on tunnistaa suojatun yhteyden osapuolet. SSH-salausprotokollan avulla käyttäjä on mahdollista tunnistaa kolmen eri tunnistusmenetelmän avulla. Se voidaan tunnistaa joko:

- käyttäjänimen ja salasanan perusteella,
- käyttäjänimen ja julkisen avaimen perusteella tai
- käyttäjänimen ja työaseman perusteella

(Ruohonen 2002, 288)

Yhteyskerros mahdollistaa erillisten kanavien muodostamisen siirtokerroksen sisälle. Näitä avattuja kanavia voidaan käyttää joko pääte-yhteyteen tai yhteyden välittämiseen eli tunneloimiseen. Joten esim. palvelin voi toimia kahden työaseman viestien välittäjänä. (Ruohonen 2002, 289)

4.2.2.5 SSL

SSL (Secure Socket Layer) on salausprotokolla, joka toimii lähes samalla tavalla kuin SSH-protokolla. SSL jakaa toimintansa kahteen eri protokollaan: Handshake protocol ja Record Layer. Handshake procol eli kättelemisprotokollan tehtävänä on sopia käytettävästä salakirjoitusmenetelmästä asiakkaan ja palvelimen välillä. Tarvittavat osapuolien tunnistamiset suoritetaan kättelyvaiheessa erilaisilla sertifikaateilla. Record Layer-protokolla huolehtii viestien osioimisesta, pakkaamisesta, salakirjoittamisesta ja eheyden varmistamisesta. (Ruohonen 2002, 289-290)

SSL-protokollan avulla on mahdollista muodostaa salattuyhteys ilman erillistä asiakasohjelmistoa. Salatun yhteyden muodostaminen onnistuu miltä tahansa Internetiin kytketyltä työasemalta. Yhteys muodostetaan Internet-selaimen ja sen käyttämän SSL-salauksen avulla. (Ruohonen 2002, 289)

SSL-protokollaa voidaan käyttää seuraavilla protokollilla:

- HTTPS-protokolla: HTTP-protokolla salattuna SSL-protokollalla, www-selaus
- SSMTP-protokolla: SMTP-protokolla salattuna SSL-protokollalla, sähköposti
- NNTPS-protokolla: NNTPS-protokolla salattuna SSL-protokollalla, uutisryhmät
- FTPS-protokolla: FTP-protokolla salattuna SSL-protokollalla, tiedostojen siirto
- Telnets-protokolla: Telnet-protokolla salattuna SSL-protokollalla, pääte-yhteys

(Ruohonen 2002, 289)

4.2.3 VPN-ratkaisut

Erilaisia VPN-ratkaisuja on markkinoilla tarjolla monenlaisia. Ne voidaan jakaa kahteen kategoriaan: ohjelmistopohjaisiin- ja laitteistopohjaisiin ratkaisuihin. Näiden em. lisäksi on olemassa myös niiden erilaisia yhdistelmiä.

4.2.3.1 Ohjelmistopohjaiset VPN-ratkaisut

Ohjelmistopohjaisen VPN-ratkaisun perusajatuksena on yhdistää etäkäyttäjän tietokone yrityksen verkkoon ja sen resursseihin turvallisesti, käyttämällä jo yrityksen verkossa olevia laitteita ja ohjelmistoja. Ohjelmistopohjaiset ratkaisut voidaan jakaa kahteen kategoriaan: palomuurit sekä toimintaspecifiset ohjelmistot. (Perlmutter & Zarkower 2001, 142)

Palomuurien tehtävänä on suodattaa paketteja yrityksen verkon ja julkisen verkon välillä. Nykypäivänä palomuurien tehtävät ovat lisääntyneet pelkästä pakettien suodatuksesta erilaisiin turvallisuustoimintoihin. Nykyään palomuurit pystyvät autentikoimaan yksittäisiä paketteja, käyttäjiä, istuntoja ja sovelluksia. Ne voivat tarjota lisäksi välipalvelin eli proxy-palveluja, kääntää osoitteita, salata dataa jne. Viimeisin palomuureihin lisätty ominaisuus on mahdollisuus tuottaa VPN-verkkoja. Tämän vuoksi VPN-yhteyksiä voidaan muodostaa pelkästään kahden palomuurin välille. Toinen mahdollisuus muodostaa VPN-yhteys palomuurin avulla on asentaa etäyhteyskoneeseen asiakasohjelma, jonka avulla otetaan yhteys yrityksen palomuuriin. (Perlmutter & Zarkower 2001, 142-147)

Toimintaspecifiset ohjelmat sisältävät kaksi osatekijää; asiakkaan ja palvelimen. Asiakasohjelmisto asennetaan työasemaan, jota käytetään etätyöskentelyyn ja palvelinsovellus asennetaan palvelimeen, johon luodaan VPN-yhteys. Tämä ratkaisu muodostaa VPN-yhteyden kahden tietokoneen välille. (Perlmutter & Zarkower 2001, 147-148)

4.2.3.2 Laitteistopohjaiset VPN-ratkaisut

Laitteistopohjaiset VPN-ratkaisut on suunniteltu pääasiassa kahta erilaista käyttöä varten, kuten yleistarkoituksellisiin- ja toimintaspesifisiin laitteistoratkaisuihin.

Reitittimet ovat yleistarkoituksellisia laitteistoalustoja, joiden ”älykkyys” on peräisin sen ohjelmistosta. Yleisesti myös VPN-ominaisuudet on toteutettu ohjelmallisesti reitittimiin. Reitittimiin on myös mahdollisuus lisätä VPN-teknologiaa, kuten IPSec – ja L2TP-tunnelointiprotokollat. Reitittimiä voidaan käyttää toimipaikkojen välisissä VPN-yhteyksissä sekä etäkäyttö-VPN:ssä. (Perlmutter & Zarkower 2001, 150-151)

Toimintaspesifiset laitteistoratkaisut on suunniteltu juuri VPN-sovelluksia varten. Niiden tärkeimpänä ominaisuutenaan on VPN-tunnelointi ja salaus. Lisäksi ne sisältävät joukon erilaisia turvallisuusominaisuuksia, kuten sisäänrakennettu suodatus, reititys, tuki käyttäjätason todennukselle ja käyttäjäkäytännöille jne. Toimintaspesifiset laitteistot ovat suunniteltu vain yhtä tarkoitusta varten: kriittisiä palveluita. Kriittiset palvelut koostuvat salauksesta ja lukuisten istuntojen turvallisuusliittojen isännöinnistä. (Perlmutter & Zarkower 2001, 155-156)

4.3 Tiedon salaus

4.3.1 Salausalgoritmit

Salausalgoritmeillä voidaan salata jo olemassa olevaa tietoa, tai reaaliaikaisesti sitä mukaan, kuin tietoa luodaan. Nopeasti salattava tieto vaatii salausalgoritmilta nopeutta, joten se tulee salata jonosalaajalla. Jo olemassa olevaa tietoa voidaan salata käyttäen mitä tahansa algoritmia. Algoritmit jaetaan julkisen- ja salaisen avaimen menetelmiin eli asymmetrisiin ja symmetrisiin. (Ruohonen 2002, 274)

4.3.2 DES

DES (Data Encryption Standard) on vanha ja yhä käytössä oleva salausalgoritmi. Se käyttää neljää erilaista salausmoodia (ECB, CBC, CFB ja OFB). DES-algoritmin avulla voidaan tietoa salata hyvin nopeasti, koska se käyttää salauksessa korvaus- ja virtasalaus tekniikoita sekä 64-bittisiä lohkoja ja 56-bit tistä avainta. DES-salausalgoritmi pystyttiin murtamaan vuonna 1998. DES-algoritmi on symmetrinen menetelmä (Ruohonen 2002, 274)

3-DES (Triple-DES)-algoritmi parantaa DES-algoritmin turvallisuutta salakirjoittamalla viestin monta kertaa peräkkäin eri avaimilla; 3-DES- algoritmi salaa viestin kolme kertaa peräkkäin käyttämällä kahta tai kolmea avainta. Tämän vuoksi se on hieman hitaampi kuin DES-algoritmi. 3-DES-algoritmi on symmetrinen menetelmä. (Ruohonen 2002, 274)

4.3.3 RSA

RSA-salausalgoritmi on tällähetkellä suosituin salakirjoitusalgoritmi. Sen nimi on johdettu kehittäjiensä nimistä Ron Rivest, Adi Shamir ja Leonard Adleman. RSA-algoritmin salaus perustuu diskreetin logaritmin ongelmaan sekä suurten lukujen tekijöihin jakamisen vaikeuteen. RSA käyttää 1024-4096 -bittisiä avaimia ja se on siirtosalaaja, joten se on hidas algoritmi. Toisaalta RSA on kuitenkin turvallinen; se on julkaistu jo vuonna 1978, mutta sitä ei ole vielä pystytty murtamaan. RSA on julkinen avaintensopimisalgoritmi eli asymmetrinen. (Ruohonen 2002, 275-276)

4.3.4 IDEA

IDEA (International Data Encryption Standard) käyttää samoja salausmoodeja kuin DES-algoritmi, mutta se salaa viestin 64-bitin lohkoissa ja käyttää 128-

bittistä avainta. IDEA onkin hieman kehittyneempi salausalgoritmi kuin DES ja se on myöskin symmetrinen menetelmä. (Ruohonen 2002, 276)

4.3.5 Blowfish

Blowfish on korvaussalaaja, joka käyttää 64-bitin lohkoja ja 448-bittistä avainta. Se käyttää salaukseen kuuttatoista salauskierrosta, mutta ennen salausta avaimesta täytyy muodostaa 4168-tavua pitkä avain, jota käytetään salaukseen. Blowfishin salaus tapahtuu 32-bittisellä prosessorilla. Lisäksi se on symmetrinen, eli se käyttää salaisen avaimen menetelmää. (Ruohonen 2002, 276)

4.3.6 AES

AES (Advanced Encryption Standard) on kehitetty korvaamaan DES-algoritmi. AES-algoritmi käyttää Rijndael-algoritmia ja se käyttää 128-, 192- tai 256-bittistä avainta. Lohkon koko on myös vastaavasti 128-, 192- tai 256-bittiä. AES-salausalgoritmi toimii taulukointiperiaatteella. Selväkielinen sanoma lohkotaan ja sen lohkot sijoitetaan omiin taulukoihinsa salakirjoitusavaimen kanssa. Taulukoissa on neljä riviä ja sarakkeet lasketaan jakamalla lohkon tai avaimen pituus 32:lla (bitteinä). Taulukkoa täytetään lohkon tai avaimen tavuilla sarake kerrallaan. Rijndael-algoritmi käyttää useaa salauskierrosta, joiden lukumäärä valitaan sarakkeiden perusteella. Jokaiselle salakierrokselle muodostetaan kierrosavaimet ja lisäksi samalla muodostetaan kierrosavain ylimääräiselle kierrokselle, joka tehdään viimeiseksi. (Ruohonen 2002, 278)

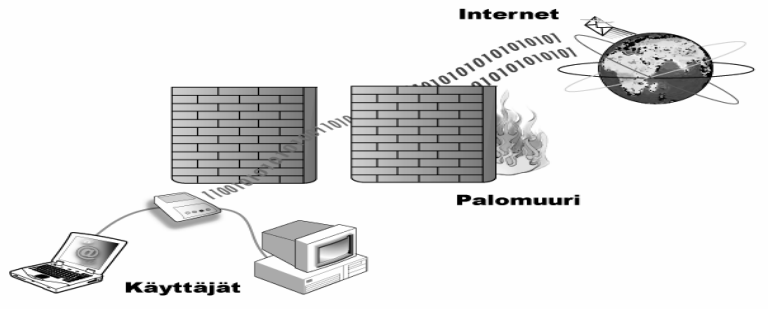
4.4 Diffie-Hellman-protokolla

Diffie-Hellman-protokollaa käytetään, kun lähetetään salaista tietoa. Se on avaintensopimisprotokolla, jonka avulla lähettäjä ja vastaanottaja sopivat

käytettävästä salaisesta avaimesta ilman datan lähetystä. Lähettäjän ja vastaanottajan avaintensopiminen perustuu lukujen laskemiseen. Kumpikin osapuoli laskevat vähintään 150 numeroa pitkistä satunnaisluvuista, yhteisen avaimen. Diffie-Hellman-protokollaa käytetään muiden todennusmenetelmien kanssa suojaamaan IP-liikennettä. Se on julkinen avaimenvaihtoprotokolla. (Ruohonen 2002, 286)

4.5 Palomuuri

Palomuuri (firewall) on laite, joka suodattaa julkisen ja suojattavan verkon välistä liikennettä. Palomuurilaitteet sisältävät tiettyjä ennalta määritettyjä sääntöjä, joiden perusteella se tarkkailee verkkoliikennettä. Yrityksen sisäverkkoon kohdistuvasta liikenteestä se suodattaa kaiken ylimääräisen pois, ja päästää vain tarvittavan liikenteen verkkoon. (Palomuuri)



KUVIO 2. Havainnollistaa palomuurin toimintaa. (Palomuuri)

Pakettisuodatuspalomuuri (Packet filtering) eli tilaton palomuuri tuhoaa kaiken ylimääräisen liikenteen, joka on suodatussääntöjen (Filter rule) vastaista, joten säännöt näyttelevät palomuurin tärkeintä osaa. Pakettisuodatuspalomuuri suodattaa liikenteen pakettien kuvauksien eli otsikkotietojen perusteella. Näitä otsikkotietoja voivat olla seuraavat asiat:

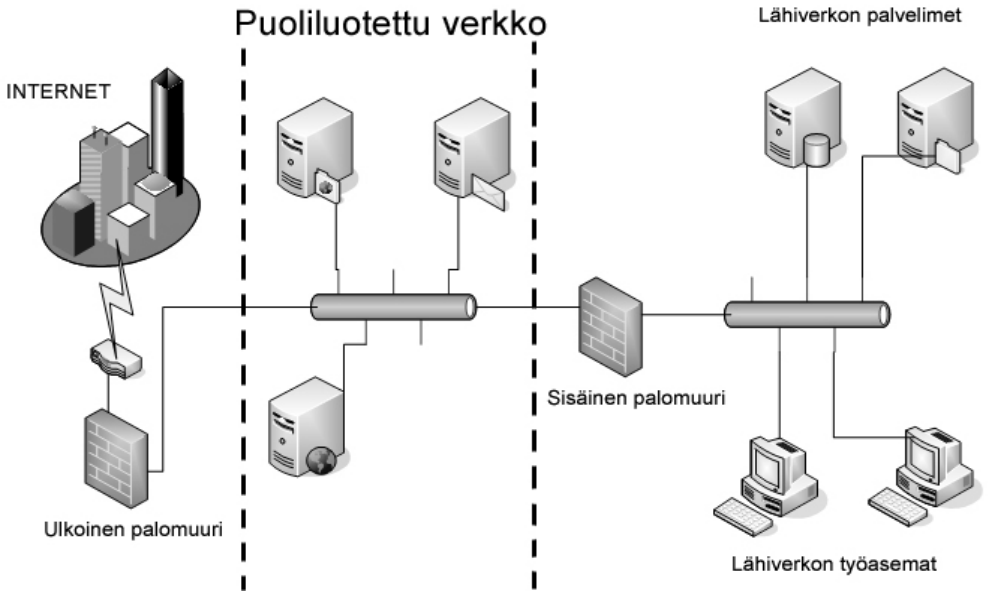
- paketin lähdeosoite ja lähdeportti
- paketin kohdeosoite ja kohdeportti
- paketin protokolla

- ICMP-paketin tyyppi ja koodi
- paketin liput
- kellonaika, jolloin sääntö on voimassa

(Ruohonen 2002, 64-66)

Tilallinen pakettisuodatus palomuuri (stateful filtering) perustuu aikaisempien yhteyksien tarkkailuun, joten se päättää aikaisemman yhteyden perusteella tuhotaanko paketti, vai sallitaanko liikenne sisäverkkoon. Tämän vuoksi suojaamattoman verkon ulkopuolella olevat tietokoneet eivät voi muodostaa yhteyttä verkkoon, jossa on tilallinen pakettisuodatuspalomuuri, ellei suojatunverkon sisäpuolella oleva tietokone lähetä vastauksia ulkopuolelta tuleviin paketteihin. (Ruohonen 2002, 70-71)

Jotta etätyöasema voisi muodostaa yhteyden palomuurin takana olevaan palvelimeen, täytyy palomuuriin tehdä omat säännöt yhteyttä varten tai vaihtoehtoisesti palvelimille voidaan luoda puoliluotettu verkko(DMZ, DeMilitarized Zone). Windows 2000 verkoissa verkkojen eri osien välille sijoitetuissa palomuureissa täytyy sallia myös LDAP-protokolla (UDP-protokolla, portti 389), jotta Active Directory eli hakemistopalvelu toimisi. (Ruohonen 2002, 73-75)



KUVIO 3. Puoliluotetun verkon kokoonpano. (DMZ)

4.6 Käyttäjäntunnistaminen

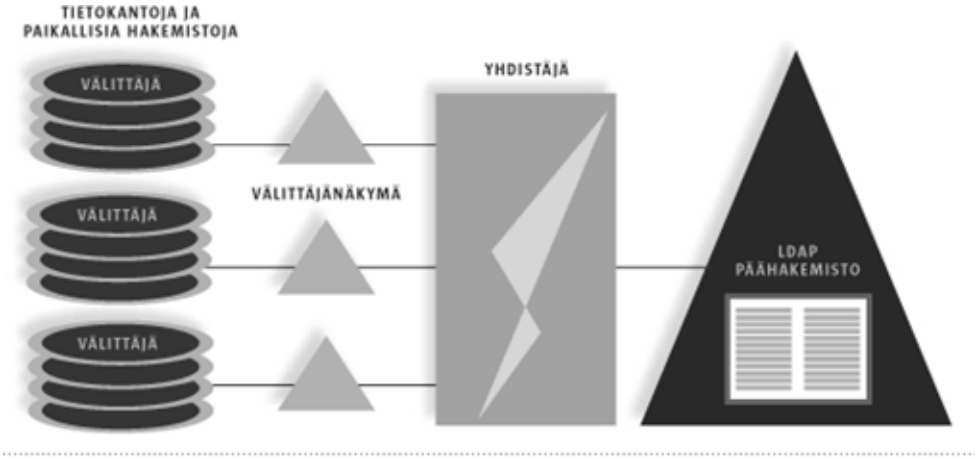
4.6.1 Hakemistopalvelu

Hakemistopalvelu (directory service) on eräänlainen tietokanta, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Hakemistopalvelu mahdollistaa keskitetyn päähakemiston, jonka avulla voidaan jakaa resursseja käyttäjille ja sovelluksille. Käyttäjä voidaan luoda vain kerran yhdellä käyttöliittymällä, ja käyttäjä vaihtaa salasanansa yhdestä käyttöliittymästä, jonka jälkeen salasana vaihtuu välittömästi kaikille sovelluksille. Lisäksi hakemistopalvelun avulla voidaan selkeällä tavalla nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja. Hakemistopalvelu noudattaa asiakas/palvelin-arkkitehtuuria ja se tarjoaa verkkoprotokollan näitä yhteyksiä varten (LDAP). (Active Directory)

Hakemistopalvelu (Active Directory) on sisälletty Microsoft Windows Server 2000:een ja Microsoft Windows Server 2003:een.

4.6.2 Metahakemisto

Metahakemisto on yksi hakemisto, johon on yhdistetty tietoa monesta eri hakemistosta. Metahakemisto helpottaa tilannetta, jossa työntekijällä on monia erilaisia salasanoja ja muuta tietoa (mm. puhelinnumero, sähköpostiosoite) monessa eri tietokannassa tai hakemistossa. Metahakemiston avulla voidaan kerätä kaikki tiedot yhteen LDAP-hakemistoon. Tämä helpottaa työntekijän tietojen ylläpitoa. (Metahakemisto)



KUVIO 4. Metahakemiston komponentit (Metahakemisto)

Kuviossa 4 on nähtävissä metahakemiston komponentit, jotka ovat osallisena tiedon keruussa LDAP-hakemistoon. LDAP-hakemiston ”aivoina” toimii yhdistäjä, joka yhdistää eri tietokantojen ja hakemistojen tiedot yhteen LDAP-hakemistoon, jota kutsutaan metahakemistoksi. Se myös määrittää miten tiedot yhdistetään, miten ne päivitetään ja mihin kantoihin. (Metahakemisto)

4.6.3 LDAP-hakemistoprotokolla

LDAP (Lightweight Directory Access Protocol) on hakemistoprotokolla, joka on yleistymässä keskitetyn hakemiston protokollana. LDAP-hakemistoprotokolla toimii TCP/IP-verkoissa ja se määrittelee hakemistoon kohdistuvat operaatiot ja tavan kuinka ne suoritetaan. Lisäksi LDAP-protokolla sisältää informaatiomallin ja nimiavaruuden. Informaatiomalli määrittää informaation rakenteen ja tyypin, kun taas nimiavaruus määrittää miten informaatioon viitataan ja kuinka se on organisoitu. (LDAP)

LDAP-protokollaa käytetään pääasiassa käyttäjien autentikointiin ja sitä tuetaan hyvin laajasti. Toisaalta LDAP-protokolla versio 2:n pahimmat puutteet koskevat juuri tietoturvaa ja kansainvälisiä merkistöjä. Salasanan täytyy olla selvämerkkinen ja se käyttää Kerberos versio 4:ää. Kerberos on tunnistusprotokolla joka on Kerberos palvelimien käytössä. Uuden LDAP-

protokollan päivityksen myötä siihen on lisätty SSL-protokolla, sekä muita tietoturvaominaisuuksia. (LDAP)

4.6.4 RAS-palvelin

RAS-palvelin (Remote Access Service) on palvelin, jonka soittosarjaan käyttäjä soittaa modeemillaan. Käyttäjä tunnistetaan käyttäjätunnuksen ja salasanan perusteella, jonka jälkeen käyttäjän on mahdollista lähettää ja vastaanottaa paketteja kyseisen soittosarjan verkosta. Käyttäjän ja soittosarjan välille muodostuu tunneli joka salataan salaus protokollalla esim. PPP-protokollalla. Todellisuudessa RAS vain kommunikoi etäkäyttäjä-asiakkaan kanssa, mutta ei suorita autentikointia. Koska samalla yrityksellä (tai yleisemmin toimialueella, jonne pääsystä on kyse) on useita RAS-palvelimia, nämä tarkistavat etäkäyttäjän autentisuuden erilliseltä autentikointipalvelimelta. (Ruohonen 2002, 96)

4.6.5 RADIUS-palvelin

RADIUS -protokolla (Remote Authentication Dial In User Service) on suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen. RADIUS protokolla käyttää hyväkseen asiakas/palvelin -mallia jolloin RADIUS on asiakas ja salasanapalvelin on palvelin. Tällöin RADIUS-protokolla välittää saadut käyttäjätiedot palvelimelle, joka hakee käyttäjän tiedot tietokannasta. Käyttäjätunnusten ja muiden käyttäjätietueiden ollessa oikein RADIUS-palvelin päästää käyttäjän verkkoon saamien asetusten ja käyttöoikeuksien mukaan.(Radius-protokolla)

RADIUS-palvelin saattaa pitää sisällään tietokannan käyttäjistä, mutta se osaa myös käyttää hyväkseen hakemistopalveluita kuten Windows 2000 Active Directory:ä ja Novell eDirectory:ä. (Radius)

4.6.6 Kerberos-todennusprotokolla

Kerberos on todennusprotokolla, jota käytetään käyttäjien henkilöllisyyden tunnistamiseen verkkojen yli Internetissä ja lähiverkoissa. Käyttäjien todennuksen lisäksi Kerberos estää salakuuntelun ja tunnistaa, jos viestiä on muokattu matkalla. Kerberos-järjestelmään kuuluu hallintopalvelin (KADM, Kerberos Administration Server), autentikointipalvelimia (AS, Authentication Server), joukko lipukkeenmyöntämispalvelimia (TGS, Ticket-granting Server) sekä palvelimia jotka tunnistavat käyttäjän. Kerberos-järjestelmä perustuu tietokantoihin, joihin on tallennettu kaikkien käyttäjien- ja palvelimien nimet, sekä tarvittavat avaimet. Lisäksi kannassa voi olla muita tunnistamiseen vaikuttavia tekijöitä. (Ruohonen 2002, 278)

Käyttäjän halutessa kirjauta Kerberos-järjestelmään, on käyttäjän vastaanotettava autentikointipalvelimelta eräänlainen valtakirja, joka sisältää TGT-lipukkeen. TGT-lipuke sisältää käyttäjän avaimella salakirjoitetun istuntoavaimen lisäksi erilaisia tietoja käyttäjästä, kuten mm. alueen johon käyttäjä kuuluu, käyttäjän nimen, osoitteet työasemista joissa lippua voi käyttää jne. Kun valtakirja on vastaanotettu, käyttäjä pyytää TGS-palvelimelta uutta lipuketta palvelimelle, johon haluaa kirjautua. Käyttäjän pyyntö sisältää TGT-lipukkeen sekä käyttäjän tunnistimen, jotka ovat salakirjoitettu istuntoavaimella. TGS-palvelin ottaa vastaan käyttäjän lähettämän pyynnön ja purkaa salakirjoituksen sekä TGT-lipukkeesta että tunnistimesta. TGS-palvelimen hyväksyessä käyttäjän pyynnön kirjautumisesta tietylle palvelimelle, se luo käyttäjälle lipukkeen jonka avulla käyttäjä on oikeutettu kirjautumaan palvelimelle. Tämä TGS-palvelimelta saatu uusi lipuke on salakirjoitettu sen tietyn palvelimen avaimella, johon käyttäjä haluaa kirjautua. Uuden lipukkeen lisäksi käyttäjä saa uuden istuntoavaimen, jonka avulla käyttäjä salakirjoittaa uuden tunnisteen. Käyttäjä lähettää pyynnön palvelimelle, johon haluaa kirjautua ja liittää pyyntöön luomansa tunnisteen ja TGS-palvelimelta saadun lipukkeen. Palvelin tarkistaa tunnisteen ja lipukkeen, joiden avulla se päättää käyttäjän oikeudesta kirjautua palvelimelle. (Ruohonen 2002. 279-284)

4.7 Tietoliikenneyhteydet

Tietoliikenne tietokoneiden yhteydessä tarkoittaa datan siirtämistä paikasta toiseen, eli kahden tietokoneen välistä kommunikointia keskenään. Tämä asettaa tietokoneille tiettyjä vaatimuksia, kuten tietoliikennesovittimen, tietoliikenneohjelman ja siirtotien, jota pitkin tieto voi liikkua. Data eli tieto voi sisältää tekstiä, kuvaa, ääntä tai liikkuvaa kuvaa, jotka on muunnettu bittimuotoiseksi. Tietoliikennettä voi kuvata parhaiten normaalin kirjeen lähettämisellä, sillä tietoliikenteessä tarvitaan samoja asioita: tarvitaan lähettäjä, vastaanottaja, itse lähetettävä viesti (data) sekä kanava, jota pitkin viesti voidaan siirtää. (Paananen 2003, 198)

4.7.1 Modeemi

Modeemin tarkoituksena on siirtää dataa puhelinlinjoja pitkin toisiin laitteisiin. Sen toimintaperiaate on hyvin yksinkertainen: modeemi muuntaa siirrettävän datan ääneksi, jonka se lähettää puhelinlinjaa pitkin toiselle modeemille, jota vastaanottava laite kuuntelee ja purkaa äänen takaisin dataksi. Puhelinlinjat ovat hyvin herkkiä häiriöille, josta johtuen modeemien nopeudet voivat kärsiä niistä. Modeemia käytettäessä on syytä muistaa, että puhelinlinja on tällöin varattu vain modeemille. (Syrjänen 1995)

Modeemit jaetaan kahteen päätyyppiin: sisäisiin- ja ulkoisiin modeemeihin. Ulkoinen modeemi yhdistetään tietokoneen sarjaporttiin, ja sisäinen modeemi asennetaan tietokoneen sisälle sille sopivaan korttipaikkaan. Tiedonsiirto ominaisuuksiin modeemin tyypillä ei ole vaikutusta. Modeemien tiedonsiirtonopeudet ovat 1 200 – 56 600 b/s. (Syrjänen 1995)

4.7.2 ISDN

ISDN (Integrated Services Digital Network) on nopeampi vaihtoehto pelkälle modeemille. ISDN ei varaa puhelinlinjaa, vaan tietokoneen ohella on mahdollista käyttää myös puhelinta. Kotikäyttäjille on suunnattu kaksi kappaletta 64 000 b/s kanavaa sekä yksi merkinantokanava, joka mahdollistaa 128 000 b/s nopeuden. Yritysten käyttöön ISDN mahdollistaa 30 kanavaa ja tämän kokonaissiirtokapasiteetti on 2 Mbit/s. (ISDN- Mitä se on?)

ISDN-yhteyttä varten on asennettava erityinen verkkopääte, johon kytketään puhelimet, faxit ja muut tietoliikennelaitteet. Tietokoneeseen täytyy myös asentaa tietoliikennelaite, joka huolehtii tiedonsiirrosta ja ISDN-yhteydestä. (ISDN- Mitä se on?)

4.7.3 ADSL

ADSL (Asymmetric Digital Subscriber Line) on nykyaikainen puhelinlinjaa käyttävä tiedonsiirtoyhteys, joka mahdollistaa useiden megabittien sekuntinopeuden. ADSL-yhteys vaatii erityisen ADSL-modeemin, joka yhdistetään puhelinlinjaan. ADSL Internet-yhteys on epäsymmetrinen, joten Internet-palvelimelta tuleva tiedonsiirtonopeus on huomattavasti nopeampi kuin käyttäjältä palvelimelle päin. Vaikka ADSL-yhteys käyttääkin puhelinlinjaa, niin puhelinta voi käyttää aivan normaalisti tietoliikenneyhteyden ollessa auki. ADSL-yhteys käyttää puhelinlinjan korkeita taajuuksia, jotka eivät häiritse normaalia puhelinliikennettä. Puhe ja data kulkevat puhelinlinjaa pitkin puhelinkeskukseen, josta puhe välitetään eteenpäin puhelinverkkoon, ja data siirretään DSL-keskittimen kautta Internet-verkkoon. ADSL-yhteyden nopeuteen vaikuttaa huomattavasti puhelinkeskuksen etäisyys ADSL-modeemista. (ADSL, kodin nopea yhteys internetiin)

ADSL-yhteyden peitto on Suomessa 98 %:lla kunnista, mutta vain noin puolella suomalaisista on mahdollisuus ADSL-yhteyteen, sillä haja-asutusalueiden ja

taajama-alueiden välillä on eroja. Suomessa kotitalouksilla on tyypillisesti käytössä nopeudet 258 kb/s -1 Mb/s. (ADSL, kodin nopea yhteys internetiin)

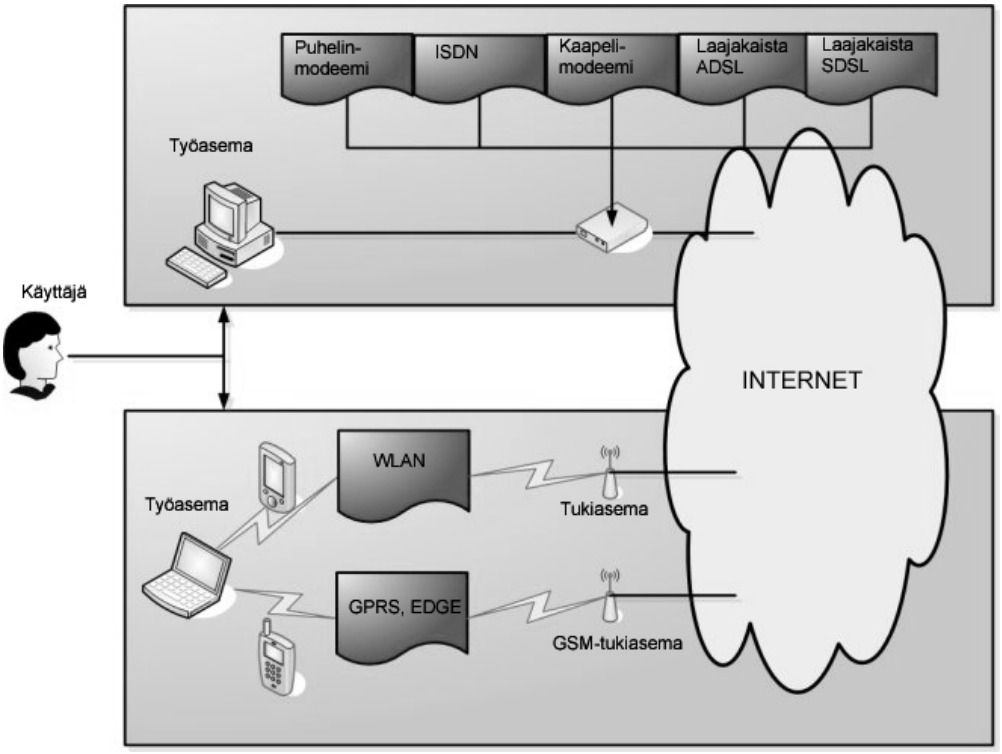
4.7.4 Kaapelimodeemi

Kaapelimodeemi toimii kaksisuuntaisessa kaapelitelevisioverkossa. Sen avulla voidaan tietokoneeseen yhdistää laajakaistainen Internet-yhteys. Kaapelimodeemi asennetaan tietokoneen ja kaapelitelevisioverkon väliin, jolloin antennijohto tuodaan television antennirasiasta kaapelimodeemiin, ja Ethernet-kaapeli kytketään modeemista tietokoneeseen. Tätä varten tietokone tarvitsee verkkokortin. (Kaapelimodeemi)

Euroopan unionissa, OECD:ssä ja ITU:ssa on annettu asetus, jonka mukaan kiinteissä yhteyksissä minimi tiedonsiirtonopeus on 256 kbit/s, mutta Suomessa yleisin tiedonsiirtonopeus on 2 Mbit/s. (Mikä on laajakaista?)

4.7.5 Muut yhteydet

Nykyään on tarjolla monia erilaisia yhteyksiä, niin yrityksille kuin yksityisillekin henkilöille. Käytettävän tiedonsiirtoyhteyden ratkaisee laite, jolla yhteys halutaan saada. Erilaiset langattomat yhteydet kannettavientietokoneiden, käsimikrojen, matkapuhelimien ja palveluntarjoajien välillä ovat yleistymässä niiden kehittymisen ja yhteiskunnan mobilisoitumisen myötä. Langattomiayhteyksiä ovat mm. WLAN (Wireless Local Area Network), GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for GSM Evolution) ja 3G-verkot, jotka kehittyessään takaavat nopean ja turvallisen yhteyden maailmalle.



KUVIO 5. Erilaisia tietoliikenneyhteyksiä Internetiin. (Internet)

5 SYMANTEC PCANYWHERE 11.5

5.1 Perusesittely

PcAnywhere on Symantec-yhtiön luoma etäkäyttöohjelmisto. Symantec on tuttu virusohjelmistojen ja muiden tietoturvaohjelmistojen tuottaja. PcAnywhere toimii Windows-pohjaisella (98/NT/ME/2000/2003 Server/XP) alustalla ja se on kahden työaseman välinen työkalu jolla voidaan siirtää, tulostaa ja muokata tietoa, sekä sen avulla voidaan muuttaa tietokoneen asetuksia. (Symantec pcAnywhere User´s Guide, 13-15)

Symantec PcAnywhere etäkäyttöohjelmisto vaatii ohjelman asennuksen molemmille työasemille, jotka mahdollistavat yhteyden muodostamisen työasemien välille. Yhteyden luonti tapahtuu asentamalla toinen työasema host-tilaan ja toinen remote-tilaan. Host-tilassa oleva tietokone on ns. isäntäkone, josta tieto haetaan ja remote-tilassa oleva kone on yhteydenottava kone. Jotta yhteyden luonti työasemiin onnistuu, täytyy molempien työasemien olla käynnissä. (Symantec pcAnywhere User´s Guide, 15)

Host-tilassa olevaan tietokoneeseen voidaan yhdistää useampiakin (Remote-työasemia) työasemia etäyhteydellä. Tämä vaatii Host-tilassa olevalta koneelta määrityksiä etätyöasemista, joilla on oikeus kirjautua koneeseen.

PcAnywhere-ohjelmisto käyttää muista etäkäyttöohjelmistoista tuttua ominaisuutta, jossa esim. käytettävän ohjelman suoritus tapahtuu ainoastaan isäntäkoneella. Lisäksi vain näppäimistön ja hiiren komennot sekä tietokoneen näytön informaatio siirtyy isäntäkoneen ja etäyhteyskoneen välillä tietoliikenneyhteyden avulla. Etäkäytöllä on mahdollista päästä käsiksi Host-koneen verkkoresursseihin. (Symantec pcAnywhere User´s Guide 15-16)

5.2 Käyttökohteet

PcAnywhere:ä voidaan käyttää seuraavissa tehtävissä:

- Erilaiset asiantuntijatehtävät. Helpdesk-, verkko- ja IT-asiantuntijat voivat etäyhteyden avulla ratkaista ongelmia, koska etäyhteyttä käyttämällä voidaan esim. tarkastella toisen henkilön tietokoneen työpöytää ja asetuksia.
- Verkkoasiantuntijat voivat käyttää etäyhteyttä apunaan muuttaakseen asetuksia ja ratkaistakseen ongelmia yrityksiensä erilaisissa palvelimissa.
- Tiedostojen siirto toimiston koneelta kotikoneelle etäyhteyden avulla.
- Etätyöskentely, kuten dokumenttien tulostaminen etäkoneelta esim. kotiin, sekä tiedostojen katseleminen ja editoiminen kotoa käsin.

(Symantec pcAnywhere User´s Guide, 13-14)

PcAnywhere etäkäyttöohjelmistolla on monia erilaisia käyttökohteita, koska se mahdollistaa yhteyden tietokoneisiin, jotka ovat fyysisesti erillään joko talon sisällä tai laajemmalla alueella. PcAnywhere on kevyt ohjelma ja se toimii hitaimmillakin yhteyksillä.

5.3 Tietoliikenneyhteydet

Etäyhteys voidaan muodostaa työasemien välille seuravilla tavoilla:

- suorayhteys, sarja- tai rinnakkaiskaapeleilla
- modeemiyhteys
- verkkoyhteys

Suorayhteys on mahdollista vain silloin, kun tietokoneet ovat lähekkäin, jolloin kaapelit ylettyvät koneiden välille ja ne kytketään tietokoneiden sarja- tai rinnakkaisportteihin. Samaan verkkoon kytkettyjen työasemien välinen yhteys onnistuu IP-osoitteiden tai työasemien nimien perusteella. Jos kummallakaan tietokoneella ei ole Internet-yhteyttä, yhdistäminen tapahtuu soittamalla suoraan toiseen tietokoneeseen modeemilla. Varsin yleinen tilanne voisi olla tällainen, jossa etäyhteystietokoneella (remote) ei ole yhteyttä Internetiin, mutta siinä on käytössä modeemi- tai ISDN-yhteys. Vastaavasti isäntäkoneella on yhteys Internetiin, mutta ei käytössään modeemi- tai ISDN-yhteyttä. Tällöin etäyhteyttä muodostavan tietokoneen on soitettava modeemilla erilliseen RAS-palvelimeen tai käytettävä VPN-yhteyttä. (Symantec pcAnywhere User´s Guide, 29-31)

Yhteyden muodostaminen Internet-yhteyden avulla työasemien välille vaatii työasemilta IP-osoitteet sekä molempien tietokoneiden tulee käyttää TCP/IP-protokollaa. Verkossa olevat palomuurit estävät työasemien yhteydet, joten verkonhallitsijan (administrator) on asetettava palomuureille tiettyjä sääntöjä. Sääntönä voisi olla esim. että vain tietty IP-osoite palomuurin takana on oikeutettu

ottamaan vastaan julkisesta verkosta tulevaa liikennettä. (Symantec pcAnywhere User´s Guide, 31-32)

5.4 Tietoturva

5.4.1 Käyttäjän tunnistaminen

PcAnywhere mahdollistaa etäyhteyden vain kun toinen tietokone on asennettu tilaan (eli host-tilaan), missä se on valmis etäyhteyden muodostukseen. Tämän vuoksi PcAnywheressä käyttäjä täytyy autentikoida jotta ylimääräiset osapuolet eivät pääse tietokoneen resursseihin käsiksi. (Symantec pcAnywhere User´s Guide, 95-96)

Verkkoympäristössä PcAnywhere mahdollistaa erilaisten autentikointimenetelmien käytön. Käyttäjäntunnistukseen käytettävä menetelmä riippuu käytössä olevasta verkkoympäristöstä. PcAnywhere mahdollistaa hakemistopalvelun käytön verkkoympäristössä yhdessä LDAP-protokollan kanssa. Hakemistopalvelun avulla voidaan käyttäjänimet ja salasanat varmistaa verkon tietokannoista. (Symantec pcAnywhere User´s Guide, 96)

Microsoft-järjestelmiin pohjautuvat verkot:	**Käyttäjän tunnistaminen:**
ADS käyttäjän tunnistaminen	Määrittelee käyttäjän Active Directory Service:stä
Microsoft LDAP käyttäjän tunnistaminen	Määrittelee käyttäjän LDAP-yhteensopivasta tietokannasta
NT käyttäjän tunnistaminen	Määrittelee käyttäjän työasemasta tai toimialueesta
Windows käyttäjän tunnistaminen	Määrittelee käyttäjän Microsoft Network Shared Directory:stä

KUVIO 6. Käyttäjän tunnistus Microsoft-järjestelmissä.

Novell-järjestelmiin pohjautuvat verkot:	Käyttäjän tunnistaminen:
Novell Binder-tunnistus	Tunnistaa käyttäjän tarkistamalla Novell NetWare Binder:stä
NDS-tunnistus	Tunnistaa käyttäjän Novellin hakemistopalvelusta
Novell LDAP-tunnistus	Tunnistaa käyttäjän LDAP-yhteensopivasta tietokannasta.

KUVIO 7.Käyttäjän tunnistus Novell-järjestelmissä.

Internet-pohjainen tunnistus:	Käyttäjän tunnistaminen:
FTP-tunnistus	FTP-palvelin tunnistaa käyttäjän FTP-palvelusta. Käyttäjätunnus ja salasana lähetetään verkon yli selvänä tekstinä.
HTTP-tunnistus	HTTP-palvelin tunnistaa käyttäjän HTTP-palvelusta. Käyttäjätunnus ja salasana lähetetään verkon yli selvänä tekstinä.
HTTPS-tunnistus	HTTPS-palvelin tarkistaa käyttäjän HTTPS-palvelusta. Käyttäjätunnus ja salasana lähetetään verkon yli salattuna.
Netscape LDAP-tunnistus	Tunnistaa käyttäjän LDAP-yhteensopivasata tietokannasta..

KUVIO 8. Käyttäjän tunnistus Internet-yhteyden pohjalta.

Suoralla modeemi-yhteydellä käyttäjä voidaan tunnistaa ns. takaisin soitolla, jolloin etäkäyttötyöasema voidaan tunnistaa valmiiksi luodun etäkäyttönumeron avulla. Kun käyttäjä soittaa modeemilla työasemaan ”isäntä”-työasema tunnistaa numeron ja katkaisee yhteyden, sekä soittaa etätyöasemaan takaisin. (Symantec pcAnywhere User´s Guide, 101)

Palvelimen ollessa etäyhteyden kohteena voidaan etäkäyttäjille asettaa tiettyjä rajoituksia. Rajoituksilla voidaan estää palvelimen tietyt resurssit, kuten esim. levyrajoitukset joiden avulla voidaan estää käyttäjää pääsemästä tietylle levylle.

Palomuurin takana sijaitsevaan työasemaan voidaan muodostaa etäyhteys VPN-yhteyttä tai suojattua tunnelia hyväksi käyttämällä. (Symantec pcAnywhere User´s Guide, 123)

5.4.2 Tiedon salaus

PcAnywhere:n omien salausalgoritmien ja autentikointimenetelmien ohella on mahdollista käyttää myös muita turvallisuuskomponentteja, joiden avulla voidaan taata turvallinen etäyhteys ja tietojen salaus. (Symantec pcAnywhere User´s Guide, 127)

VPN-yhteyttä käytettäessä ei tiedon salausta tarvitse käyttää, mutta ilman VPN-yhteyttä PcAnywhere tukee tiedon salaukseen kolmea eri menetelmää: julkista-, salaista- ja PcAnywheren omaa salausmenetelmää. (Symantec pcAnywhere User´s Guide, 109)

PcAnywhere hyödyntää 256-bittistä AES-salausalgoritmia tietojen salaukseen. (Moonsoft)

PcAnywhere käyttää RSA SecurID-varmistusavainta yhdessä RSA ACE/Server-ohjelmiston kanssa. RSA SecurID on symmetrinen avaintenvaihtoprokolla, joka on yhdistetty tehokkaaseen algoritmiin. RSA SecurID:tä käytetään PCAnywheressä autentikointiin. (Symantec pcAnywhere Admin Guide, 124)

RSA ACE/Server on RSA SecurID-ratkaisun hallintaosa, jonka avulla tarkistetaan varmistuspyynnöt ja hallitaan keskitetysti verkkojen varmistuskäytäntöjä. LDAP-protokolla on yhteensopiva RSA-palvelimien kanssa, joten se mahdollistaa keskitetyn käyttäjätietojen hallinnan. (Symantec pcAnywhere Admin Guide, 124)

RSA ACE/Agent asennetaan host eli ”isäntä”-työasemaan ja työasema asetetaan käyttämään SecurID-autentikointimentelmää, jolloin se lähettää varmistuspyynnöt RSA ACE/Serverille. (Symantec pcAnywhere Admin Guide, 124)

6 LAPLINK GOLD 12

6.1 Perusesittely

Laplink Gold 12:n avulla voi työskennellä etänä työasemien ja palvelimien välillä. Laplink Gold 12 on hyvin samantyyppinen etäkäyttöohjelmisto kuin Symantec PcAnywhere. Laplink Gold mahdollistaa erilaisten ohjelmien käytön etätyöasemassa ja sen avulla on mahdollista käynnistää tietokone etänä. Laplink sisältää etäyhteys-työkalun lisäksi joukon muita ohjelmia, kuten kommunikointi ja virustorjuntasovellukset. Laplink Gold 12 toimii Windows (98 SE, ME, 2000, XP ja Server 2000, 2003) alustoilla. (Laplink Gold 12 User´s Guide, 10)

6.2 Käyttökohteet

Laplink Goldin ominaisuuksia:

- Tiedostojen siirto ja kopiointi työasemien välillä, sekä niiden synkronointi keskenään.
- Sisältää myös tiedostojen siirron aikaisen salauksen ja virusturvan, joka tarkkailee siirrettäviä tiedostoja.
- Laplinkin Remote Desktop-ohjelman avulla voidaan hallita myös Windowsin kehittämää Windows Remote Desktop-protokollaa, joka on integroitu Windows XP:hen, Windows 2000- ja Windows 2003 servereihin, joten Laplinkilla voidaan ottaa yhteyttä myös kyseisiin käyttöjärjestelmiin.
- Laplink tarjoaa erityisen Internet-palvelun. Internet-palveluun muodotetaan käyttäjäkohtainen tili, jota käytetään etäyhteyden muodostamiseen Internetin kautta.

(Laplink Gold12 User´s Guide, 10)

Laplink Goldia voidaan käyttää erilaisissa mikrotukitehtävissä, sillä sen avulla voidaan asentaa ohjelmia etänä, ja lisäksi se mahdollistaa Microsoftin kehittelemän Remote Desktop-protokollan käytön. Microsoftin Remote Desktop-protokolla mahdollistaa yhteyden Microsoft:n tuotteisiin. Lisäksi se sisältää joukon erilaisia ohjelmia joiden avulla etäkäyttäjä voi helposti hyödyntää etänä työaseman ja palvelimen resursseja. (Laplink Gold12 User´s Guide, 10)

6.3 Tietoliikenneyhteydet

Laplink Gold tukee monia erilaisia tietoliikenneyhteyksiä:

- USB-, sarja- ja rinnakkaiskaapeli
- lähiverkko
- modeemi
- infrapuna
- Laplink Internet-yhteys
- CAPI 2.0, ISDN

(Laplink Gold12 User´s Guide, 77-78)

Laplink Internet-yhteyttä käytettäessä on luotava käyttäjätili Laplinkin Internet-sivustolle (www.laplink.com). Käyttäjätili mahdollistaa yhteyden palomuurien, proxy-palvelimien ja reitittimien läpi ilman niihin tehtäviä muutoksia. Luotuun käyttätiliin lisätään työasemat, joihin halutaan yhteys Internet-yhteyden kautta. Tämän jälkeen on mahdollista ottaa yhteyttä käyttäjätiliin lisättyihin työasemiin. (Laplink Gold12 User´s Guide, 84) Laplink Internet-yhteys mahdollistaa koneiden yhdistämisen vaikka molemmat koneet olisivat eri palomuurilaitteiden sisällä (Laplink Gold12 User´s Guide, 88).

Lähiverkko-yhteys työasemien välillä toimii tietokoneiden nimien tai TCP/IP/IPX-osoitteiden perusteella (Laplink Gold12 User´s Guide, 86). Modeemi-yhteys muodostetaan soittamalla suoraan toiseen koneeseen tai RAS-palvelimeen. (Laplink Gold12 User´s Guide, 89)

CAPI (Common Application Programming Interface) on ohjelmointirajapinta, jota esimerkiksi faksiohjelmat käyttävät ISDN:n kanssa. Kun käytetään CAPI/ISDN-yhteys mahdollisuutta molemmissa työasemissa täytyy olla ISDN-modeemit. (Laplink Gold12 User´s Guide, 94)

6.4 Tietoturva

6.4.1 Käyttäjän tunnistaminen

Laplink tarjoaa kaksi autentikointi menetelmää: Windowsin oma autentikointimenetelmä verkkojärjestelmissä (domain) ja Laplinkin autentikointimenetelmä. Windowsin oma autentikointi perustuu Windowsin Active Directoryn (hakemisto palvelu) käyttäjätunnuksiin ja salasanoihin. Laplinkin autentikointimenetelmän avulla voidaan luoda ohjelmaan käyttäjiä (käyttäjätunnus ja salasana), jotka pääsevät kirjautumaan etäkäyttötyöasemaan. (Laplink Gold12 User´s Guide, 14-15)

Modeemi-yhteyksissä käyttäjä voidaan tunnistaa RAS-palvelimen kautta tai ns. takaisin soiton perusteella. Modeemi-yhteyksissä tietokoneen täytyy olla käynnissä. (Laplink Gold12 User´s Guide, 22) Autentikoinnin perusteella käyttäjille voidaan asettaa etätyöasemiin erilaisia rajoituksia.

6.4.2 Tiedon salaus

Laplink Internet-yhteys käyttää salaamisen SSL-protokollaa, joka mahdollistaa salatun yhteyden palomuurien ja muiden verkkolaitteiden lävitse (Laplink). Tiedon salaukseen Laplink käyttää Microsoftin kehittämää CryptoAPI:a, jota käyttämällä myöskään siirtotien ei tarvitse olla millään tavalla turvallinen, koska kaikki viestit itse ovat jo salattuja. Tällä hetkellä CryptoAPI on saatavilla

ainoastaan 32-bittisiä Windows -sovelluksia varten, mutta Microsoft aikoo julkaista sen muillekin käyttöjärjestelmille. (CryptoAPI)

VPN-yhteyttä käyttämällä tietoja ei tarvitse erikseen salata. VPN mahdollistaa turvallisen yhteyden yrityksen sisäverkkoon.

7 CITRIX METAFRAME PRESENTATION SERVER 3.0

7.1 Perusesittely

1980-luvun ja 1990-luvun vaihteessa syntyi ajatus rakentaa palvelinalusta, joka voisi ylläpitää ja jakaa ohjelmia erilaisille ”clienteille” (tietokoneille jotka ottavat yhteyttä palvelimeen). Eräs tällainen ohjelma oli Remote Access joka toimi yrityksen paikallisverkossa (LAN), johon etäkäyttäjät pääsivät käsiksi ja siten he pystyivät hyödyntämään yrityksen verkkon resursseja. (Kaplan, Wood & Reesper 2003, chapter3)

Siihen aikaan ei kuitenkaan vielä ymmärretty ohjelmistojen jakamista, mutta yrityksissä oli käytössä erilaisia yhdistelmiä Windows-pohjaisissa tietokoneissa, jotka sisälsivät paljon erilaisia ohjelmia. Lähiverkko-yhteyksien ylläpitämiseen käytettiin erilaisten Novell, Unix ja Windows NT pohjaisia palvelimia. 1990-luvulla, Citrix kehitti palvelimeen pohjautuvan järjestelmän (server-based computing), jota nykyään kutsutaan Citrix MetaFrame XP Presentation Server:ksi. (Kaplan & Wood 2003, chapter3)

Citrix MetaFrame XP Access Suite on paketti, joka täydentää Microsoft Terminal Servicen ominaisuuksia. Käytännössä Citrix MetaFrame XP ”korvaa” Microsoft Terminal Servicen. MetaFramen avulla voidaan jakaa Windows-työpöytiä myös muillekin alustoille, kuin pelkästään Windows:lle. Tämä on ylläpidollisesti ja

ajallisesti yrityksen aikaa sekä työpanosta säästävä ratkaisu, sillä sovellukset pyörivät suoraan palvelimilla ja asennuksia ei tarvitse etäkoneisiin erikseen tehdä. Lisäksi yrityksen työntekijät voivat käyttää hyödykseen minkälaista etäyhteyttä tahansa muodostaakseen yhteyden ohjelmia jakaviin palvelimiin. Citrix:llä on tarjolla erilaisia versioita PK-yrityksestä aina suuren organisaatioon. (Kaplan & Wood 2003, chapter3)

Citrixin uusimman julkaisun Feature Release 3 (FR-3) myötä MetaFramesta tuli täysin yhteensopiva Windows 2003 Serverin kanssa. Samalla Citrix muutti lisensointi periaatteitaan aikaisemmista versioista. Aikaisemmat versiot vaativat lisenssin jokaista serveriä kohden. Uuden julkaisun myötä lisensointi muutettiin sellaiseksi, että yhtä serveriryhmää kohden tarvitsee hankkia vain yksi lisenssi. Tämän muutoksen myötä lisensoinnista tuli paljon joustavampi ja toimivampi kokonaisuus sekä monessa määrin yrityksille halvempi ratkaisu, koska tarvittavien palvelimien määrää voidaan lisätä ilman uuden lisenssin hankkimista. (Kaplan & Wood 2003, chapter3)

Lisensointi MetaFrame ohjelmistoissa suoritetaan ohjelmiston yhtäaikaisen käyttäjämäärän mukaan. Lyhykäisyydessään, jos lisenssi lupaa 50 käyttäjän kirjautumisen palvelimelle, niin käyttäjä numero 51 jää sen ulkopuolelle. Tämä mahdollistaa, että työasema voi käyttää useita palveluita eri palvelimissa, mutta vain yksi lisenssi on tällöin käytössä. (Kaplan & Wood 2003, chapter3)

Citrix MetaFrame asennetaan Windows-palvelin alustalle, joten Windowsin palvelimen laitteistovaatimukset riittävät myös Citrix MetaFrame:lle. Citrix MetaFrame XP tarvitsee kuitenkin perusasennusta tai päivitystä varten laitteistolta seuraavat vaatimukset:

- 1 GB vapaata kiintolevy tilaa
- Microsoft Windows 2000 Server SP2-päivityksellä tai Windows server 2003
- Installer 2.0 (Windows 2003:ssa on automaattisesti Installer 2.0) tai Windows 2000 SP3

(Kaplan & Wood 2003, chapter3)

7.2 Tietoliikenneyhteydet

Ohjelmat välitetään työasemille ICA-työkalulla. ICA (Independent Computing Architecture) on eräänlainen asiakasohjelma (client), joka perustuu palvelimiin pohjautuvaan järjestelmään. Se on hyvin samantapainen kuin Windowsin käyttämä Microsoftin RDP (Remote Desktop Protocol) protokolla, joka on käytössä MS Terminal Service:ssä. ICA:n avulla luodaan yhteys Citrix MetaFrame palvelimeen, joka jakaa ohjelmia työasemille. (Kaplan & Wood 2003, chapter3)

ICA-pääteohjelma tukee modeemi-, ISDN-, LAN-, WLAN-, erilaisia WAN- ja Internet-yhteyksiä, sekä erilaisia verkkoprotokollia TCP/IP, SPX, NETBIOS ja IPX. ICA-protokolla mahdollistaa hyvinkin hitaat yhteydet, kuten 20 kbps verkoissa pienellä viiveellä, mutta jo 30 kbps nopeus mahdollistaa reaaliaikaiset toiminnot. (Kaplan & Wood 2003, chapter3)

Citrix MetaFramella sovelluksia voidaan jakaa myös Internet-selaimen avulla. Tällöin ICA-protokolla integroidaan osaksi selainta, joka mahdollistaa sovellusten käytön selaimen kautta. Tällöin sovellusten etäkäyttö onnistuu paikoista, joissa on käytössä Internet-yhteys. (Kaplan & Wood 2003, chapter3)

7.3 Tietoturva

7.3.1 Käyttäjän tunnistaminen

Citrix Metaframe käyttää hyväkseen Windowsin Active Directory:ä, sen avulla voidaan hallita käyttäjäryhmiä ja käyttäjiä sekä luoda uusia ja poistaa vanhoja käyttäjiä. ICA-työkalun avulla kirjaudutaan sisään metaframe palvelimeen, joka tarkistaa Active Directorystä käyttäjätunnuksen ja salasanan.

7.3.2 Tiedon salaus

Palvelimeen pohjautuvassa järjestelmässä on kaksi tapaa muodostaa tietoturvallinen yhteys: VPN-yhteys ja julkisenavaimen menetelmä (PKI) yhdistettynä SSL (Secure Socket Layer)-protokollalla. (Kaplan & Wood 2003, chapter7)

ICA-protokolla yhteydet on suojattu 128-bit avaimella RC5 (salauskoodi) RSA salausalgoritmilla. MetaFrame palvelimet käyttävät Diffie-Hellman algoritmiä 1024-bitin avaimella, käyttämällä salauskoodi RC5:ta. MetaFrame Internet-käyttöliittymän salliva MetaFrame Secure Gateway käyttää käyttäjän tunnistamiseen RADIUS:ta tai SecureID:tä. (Kaplan & Wood 2003, chapter7)

8 YHTEENVETO

Etäkäyttöohjelmistot tarjoavat henkilöstölle ja yrityksen johdolle mahdollisuuden etätyöhön ajasta ja paikasta riippumatta. Tämä astettaa ohjelmistoille vaatimuksia niin tietoturvan, kuin tietoliikenneyhteyksienkin kohdalla. Tietoturvalla on nykypäivänä tärkeää asema etäkäyttöohjelmistoa valitessa. Se voi parhaimmillaan säästää ylimääräisistä lisäinvestoinneista ja huonosti hoidettuna se voi aiheuttaa yritykselle monien miljoonien eurojen tappiot. Ohjelmistoa valitessa onkin syytä kiinnittää huomioita erityisesti ohjelmistojen tietoturvaan.

Symantec PcAnywhere ja Laplink Gold 12 ovat hyvin samanlaisia etäkäyttöohjelmistoja. Ne mahdollistavat kaikki tarvittavat tietoliikenneyhteydet aina modeemeista lähiverkkoyhteyteen. Citrix Metaframe Presentation Server tarjoaa sovelluksien etäkäyttäjille mahdollisuuden käyttää sovelluksia minkä tahansa yhteyden kautta ja millä tahansa laitteelle. Tietoliikenteen nopeudella ei etäkäyttöohjelmistojen käytössä ole suurta vaikutusta. Se vaikuttaa ainoastaan datan siirtonopeuteen etäkoneiden välillä.

Etäkäyttöohjelmien tietoturva perustuu salattuun tietoliikenneyhteyteen ja tiedon salausalgoritmeihin. Salattu yhteys etäkäyttöohjelmissa voidaan muodostaa, niin VPN-yhteyden kuin SSL-yhteyden avulla ja tiedon salaukseen voidaan käyttää julkisen- tai salaisen avaimen menetelmää. Etäkäyttöohjelmistot hyödyntävät hyvin samantasoisia salausalgoritmejä. Symantec PcAnywhere ei tarjoa erityistä ratkaisua verkkojen palomuurien läpäisyyn, joten palomuureihin on säännöillä luotava PcAnywherelle oikeudet palomuurien ohittamiseksi. Laplink Gold tarjoaa käyttäjilleen WWW-palvelun, jonka kautta muodostetaan SSL-yhteys etätyöasemaan ilman erityisiä toimenpiteitä. Citrix Metaframe käyttää ICA-protokollaa yhteyden muodostamiseen. ICA-protokolla taas hyödyntää VPN-yhteyttä.

Etäkäyttöohjelmistojen käyttäjätunnistus riippuu käytettävästä tietoliikenneyhteydestä. Pääsääntöisesti modeemien kautta etäkäyttöohjelmistoja käyttävät henkilöt voivat käyttää ”isäntä”-ohjelmien takaisinsoittomahdollisuuksia

tai yrityksen mahdollisia RAS-palvelimia käyttäjätunnistukseen. Lähiverkkoyhteyttä (kaapelimodeemi, ADSL) käyttävien käyttäjien tunnistaminen etäkäyttöohjelmistoissa suoritetaan keskitetyllä hakupalvelulla tietokannoista eli hyödyntämällä esim. Windows-verkkojärjestelmien käyttäjähallintoa.

Symantec PcAnywhere- ja Laplink Gold-ohjelmistoja voidaan käyttää monissa tehtävissä. Tehtäviin voivat kuulua erilaiset mikrotuki- ja palvelimienhallintatehtävät sekä etätyöt kotoa käsin tai yrityksen ulkopuolelta. Edellä mainituissa ohjelmissa ei ole paljoa eroa erilaisten työkalujen ja tietoturvan osalta. Ainoa haittapuoli ohjelmistoissa on etteivät ne tue unix-järjestelmiä.

Citrix Metaframe Presentation Server on tarkoitettu ohjelmistojen etäkäyttöön palvelimilta, joten se sisältää jo valmiiksi hyvät tietoturvaominaisuudet. Citrix Metaframen avulla voidaankin turvallisesti hoitaa ohjelmien jakaminen mille tahansa työasemalle ja millä tahansa tietoliikenneyhteydellä.

LÄHTEET

Active Directory [verkkodokumentti]. [viitattu 23.3.2006] Saatavissa: http://www.csc.fi/suomi/funet/ldap.html

ADSL, kodin nopea yhteys internetiin [verkkodokumentti]. [viitattu 23.3.2006] Saatavissa: http://www.ficom.fi/fi/t_tekniikka_r.html?Id=1045051770.html

CryptoAPI [verkkodokumentti]. [viitattu 23.3.2006] Saatavissa: http://www.mit.jyu.fi/opiskelu/seminaarit/ohjelmistotekniikka/cryptoapi/

DMZ [verkkodokumentti]. [viitattu 23.1.2006]. Saatavissa: http://www.elistas.net/lista/infohackers/ficheros/3/verFichero/4/dmz%20intermedial.png

Etätyö kiinnostaa [verkkodokumentti]. [viitattu 23.1.2006]. Saatavissa: http://artikkelit.monster.fi/704_FI_p1.asp

Hakala, M. & Vainio, M. 2002. Tietoverkon rakentaminen. Docendo Finland Oy, Jyväskylä.

ISDN- Mitä se on? [verkkodokumentti]. [viitattu 20.3.2006] Saatavissa: http://www.netlab.tkk.fi/opetus/s38118/s98/htyo/44/sivu1.shtml

Kaapelimodeemi [verkkodokumentti]. [viitattu 20.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/Kaapelimodeemi

Kaplan, S. Wood, A. & Reeser, T. Citrix MetaFrame Access Suite for Windows Server 2003: The Official Guide.

L2TP [verkkodokumentti]. [viitattu 23.1.2006]. Saatavissa: http://fi.wikipedia.org/wiki/L2TP

LDAP [verkkodokumentti]. [viitattu 30.3.2006]. Saatavissa: http://www.csc.fi/lehdet/atcsc/atcsc4-98/ldap.html

Laplink Gold 12 User Manual

Metahakemisto [verkkodokumentti]. [viitattu 30.3.2006]. Saatavissa: http://fi.sun.com/sunnews/newsletter/verkkolehti/asiantuntija/0104_estlander.html#sun

Mikä on laajakaista? [verkkodokumentti]. [viitattu 20.3.2006] Saatavissa: http://www.laajakaistainfo.fi/mikaon_laajakaista/

Paananen, J. 2003. Tietotekniikan peruskirja. Docendo Finland Oy, Jyväskylä.

Palomuuri [verkkodokumentti]. [viitattu 20.3.2006] Saatavissa: http://fi.wikipedia.org/wiki/Palomuuri

Perlmutter, B. & Zarkower, J. 2001. Virtuaaliset yksityisverkot. Edita Oyj, Helsinki.

Puska, M. 2000. Lähiverkkojen tekniikka. Satku-Kauppakaari, Helsinki.

Ruohonen, M. 2002. Tietoturva. Docendo Finland Oy, Jyväskylä.

Radius [verkkodokumentti]. [viitattu 1.4.2006] Saatavissa: http://www.tml.tkk.fi/Opinnot/Tik-110.350 /Tehtavat /rfc /2058_4.html

Radius-protokolla [verkkodokumentti]. [viitattu 1.4.2006] Saatavissa: http://fi.wikipedia.org/wiki/RADIUS

Syrjänen, S. 17.8.1995. Modeemien perusasiat. [verkkodokumentti]. [viitattu 12.12.2005]. Saatavissa: http://www.helsinki.fi/atk/oppaat/mod/modeemi.html

Symantec PcAnywhere User's Guide

Symantec PcAnywhere Admin Guide

VPN-verkot [verkkodokumentti]. [viitattu 5.2.2006]. Saatavissa: http://www.2kmediat.com/vpn/johdanto.asp