Antti Harmaala

Etäkäyttöympäristön toteutus

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikka ja liikenne
Tietotekniikan koulutusohjelma
Kevät 2012

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikan ja liikenteen ala	Koulutusohjelma Tietotekniikan koulutusohjelma
Tekijä(t) Antti Harmaala	
Työn nimi Etäkäyttöympäristön toteutus	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Ohjaaja(t) Tuomo Rantala
	Toimeksiantaja Ismo Talus
Aika Kevät 2012	Sivumäärä ja liitteet 47

Tämän työn tavoitteena oli toteuttaa etäkäyttöympäristö, jossa etätyöpöytäyhteyden kautta hallitaan etäkoneen ohjelmistoja, laitteita, sekä tiedostoja etäyhteyden kautta.

Työn kirjallisessa osassa esitellään taustaa etäkäytöstä ja -työpöytäympäristöistä sekä lähiverkkoteknologioista ja etäkäyttöön liittyvistä tietoturvallisuuden näkökulmista. Varsinaisessa työnsuorituksessa esitellään eräs tapa verkkoyhteyden toteuttamiseksi pääte- ja palvelinkoneen välille, sekä kuinka verkko- ja palomuuriasetukset toteutettiin määritetyssä ympäristössä. Lisäksi testattiin kolme etäkäyttöohjelmistoa, joilla yhteydelle määritellyt tavoitteet pyrittiin saavuttamaan.

Työn tuloksena saatiin muodostettua toimiva yhteys etäkäytettävän niin sanotun palvelinkoneen ja päätekoneen välille. Lisäksi ohjelmistotestaus Windowsin etätyöpöydän, TightVNC:n ja TeamViewerin välillä osoitti, että suuria eroja ohjelmistojen käytettävyydessä ei tämäntyyppisessä verkkoympäristöissä ollut. Etätyöpöytäyhteyden muodostus onnistui kaikilla testatuilla ohjelmistoilla, ainoastaan Windows-etätyöpöydän yhteydenmuodostuksessa havaittiin ongelmia, jotka liittyivät päätekoneen verkkoasetuksiin.

Kieli	Suomi
Asiasanat	Etähallinta, Etäkäyttö, Etätyöpöytä, RDP, RFB
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS
ABSTRACT

School	Degree Programme
School of Engineering	Information Technology
Author(s) Antti Harmaala	
Title Remote Access in a Local Area Network	
Optional Professional Studies Information Security	Instructor(s) Mr Tuomo Rantala
	Commissioned by Mr Ismo Talus
Date Spring 2012	Total Number of Pages and Appendices 47

The purpose of this Bachelor's thesis was to develop and test a safe remote access connection between two computers in a Local Area Network. The reason for developing and testing this type of connection was the possibility of working simultaneously with the computers, exchanging data files and using the software of the remote computers.

This thesis describes the process of making the decision of the best connection type between the two computers in the remote access network and how the network and firewall settings are optimized. There are many different kinds of remote desktop and remote access programs that use protocols such as Remote Desktop Protocol (RDP) and Remote Framebuffer Protocol (RFB). Some of these remote desktop programs were tested and compared to find the best option for the chosen network setup.

As a result of this thesis the safe connection was achieved by means of a wired local area network connection. The software test showed that the required result can be achieved in a number of ways and the margins between the tested programs are small.

Language of Thesis	Finnish
Keywords	Remote Access, Remote Desktop, Information Security
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

SISÄLLYS

SYMBOLILUETTELO

AES	Advanced Encryption Standard. Rinjdael-algoritmiin perustuva salaisen avaimen tulosalaaja
Asiakas	Client. Etäyhteyden osapuoli, joka käyttää palvelimen (server) tarjoamia palveluja. Etäkäyttäjä.
CredSSP	The Credential Security Support Provider. Protokolla, joka mahdollistaa sovelluksen turvallisen käyttäjätunnusten välityksen asiakkaalta (client) palvelimelle (server).
DES	Data Encryption Standard. Symmetrinen lohkosalaaja.
Ethernet	Yleisin lähiverkkotekniikka, joka on määritetty IEEE 802.3 -standardissa.
FTP	File Transfer Protocol. TCP-protokollan mukainen tiedonsiirtomenetelmä.
HTTP	Hypertext Transfer Protocol. WWW:n käyttämä tiedonsiirtoprotokolla
HTTPS	Hypertext Transfer Protocol Secure. Salattu HTTP-protokolla.
ICMP	Internet Control Message Protocol. Verkossa olevien laitteiden hallintaviestien lähettämiseen käytetty protokolla.
IEEE	Institute of Electrical and Electronics Engineers. Teknisten ammattilaisten yhteisö, joka vastaa muun muassa tietotekniikan ja elektroniikan suositusten ja standardien kehityksestä.
IGMP	Internet Group Management Protocol. Multicast-ryhmien hallintaprotokolla.
IP	Internet Protocol. IP-datapakattien kuljetusprotokolla.

ITU	International Telecommunication Union. Kansainvälinen televiestintäliitto
KSA	Key Scheduling Algorithm. RC4:n avainajoitusalgoritmi.
LAN	Local Area Network. Lähiverkko
LLC	Logical Link Control. OSI-mallin siirtoyhteyskerroksen ylempi osa, joka on määritetty IEEE 802.2 -standardissa.
MAC	Medium Access Control. OSI-mallin siirtoyhteyskerroksen alempi osa.
MAN	Metropolitan Area Network. Kaupunkiverkko.
OSI-malli	Open System Interconnection, tietojärjestelmien toisiinsa liittämiseen kerrosarkkitehtuurimalli.
Palvelin	Server. Etäyhteyden osapuoli, joka jakaa palveluitaan asiakkaalle, esimerkiksi näyttödataa. Etäkäytettävä yhteyden osapuoli.
Palvelinkone	Etäkäytettävä tietokone. Etäyhteysverkon palvelin.
PRGA	Pseudo-Random Generation Algorithm. RC4:n näennäissatunnaislukugeneraattori
Päätekone	Etäkäyttävä tietokone. Etäyhteysverkon asiakas.
RDP	Remote Desktop Protocol. Windowsin etätyöpöytäprotokolla.
RFB	Remote Framebuffer Protocol. Etäkäyttöprotokolla.
RLE	Run-Lenght Encoding. Tiivistysmenetelmä, jolla datan sisältämät samat peräkkäiset merkit korvataan laskurilla.
RSA	Epäsymmetrisen julkisen avaimen salausalgoritmi.
SSH	Secure Shell. Salausprotokolla
SSL	Secure Socket Layer. Salausprotokolla.
STP	Shielded Twisted Pair. Suojattu parikaapeli.
TCP	Transmission Control Protocol. Yhteydellinen kuljetusprotokolla.

TCP/IP	Transmission Control Protocol/Internet Protocol. Yhdistelmä Internet-liikennöinnin tietoverkkoprotokollista.
TSL	Transport Layer Security.
UDP	User Datagram Protocol. Yhteydettömän yhteyden tiedonsiirtoprotokolla.
UTP	Unshielded Twisted Pair. Suojaamaton parikaapeli.
VNC	Virtual Network Computing. RFB-protokollaa käyttävä etätyöpöytärjestelmä
VPN	Virtual Private Network. "Yksityinen" verkko julkisen verkon yli.

1 JOHDANTO

Tässä dokumentissa kuvataan etäkäyttöjärjestelmän toteutusta, jossa tietokonetta ja sen laitteita ja ohjelmistoja käytetään etäyhteyden kautta etätyöpöytäohjelmistolla. Lähtökohtana työlle oli tarve käyttää tietokoneita samanaikaisesti, jotta esimerkiksi tiedostojen siirto sekä etäkoneen ohjelmistojen käyttö olisi mahdollista niin sanotun päätekoneen kautta. Tyypillisimmillään etäkäytön tai -hallinnan menetelmiä käytetään työskenneltäessä tai opiskeltaessa ”etänä” varsinaisen toimipisteen ulkopuolella, sekä mikrotuen apuvälineenä. Tässä työssä tarkasteltu etäkäyttöympäristö toteutetaan kuitenkin lähiverkkoympäristössä.

Etäkäyttöympäristö sijoitetaan erääseen Kajaanin ammattikorkeakoulun opetustilaan, jossa sitä käytettäisiin lähinnä opetus- ja harjoitustarkoituksiin. Kajaanin ammattikorkeakoulu on vuonna 1992 perustettu Kajaanin kaupungin omistama liikelaitos, jossa opiskelee noin 2 000 opiskelijaa. Koulutusta tarjotaan viidellä eri koulutusalalla, 12 eri koulutusohjelmassa, joista kolme on englanninkielistä [1].

Työn tavoitteena on toteuttaa etäkäyttöön sopiva verkkoratkaisu sekä mukauttaa verkko- ja palomuuriasetukset siten, että järjestelmän toiminta ja turvallisuus olisivat riittävällä tasolla. Lisäksi vertaillaan ja testataan joitakin etätyöpöytäohjelmistoja, joilla etäyhteys olisi mahdollista toteuttaa.

2 ETÄKÄYTTÖ JA -HALLINTA

Tässä luvussa määritellään termit etäkäyttö, etätyöpöytä ja etäyhteys. Lisäksi tarkastellaan kahta ehkä yleisemmin käytettyä etätyöpöytäprotokollaa, Windowsin Remote Desktop protokollaa ja Remote Framebuffer-protokollaa.

Etäkäytöllä tarkoitetaan tietokoneen käyttöä ”etänä” esimerkiksi verkon yli. Yleensä vaatimuksena etäyhteyden muodostukseen on siihen tarkoitettu ohjelmisto ja verkkoyhteys laitteiden välillä. Tyypillisessä tilanteessa yhteys muodostetaan kotoa työpaikan tai oppilaitoksen verkkoon, jonka resursseja ja tietoja käytetään verkon yli.

Etätyöpöydästä puhutaan silloin, kun toisen tietokoneen työpöytä nähdään omalla tietokoneen näytöllä ja tätä tietokonetta voidaan käyttää kuten omaa tietokonetta [2]. Etätyöpöytäyhteydellä voidaan hallita esimerkiksi koti- tai työkonetta, vaikka varsinaisesti ei oltaisi samassa tilassa. Lisäksi etätyöpöytää voidaan käyttää mikrotuen apuna vikojen ja häiriöiden havaitsemiseen ja korjaamiseen.

Etäyhteydellä tarkoitetaan tietoliikenneyhteyttä, joka muodostetaan etäkäyttöä varten, jolloin tietokonetta tai tietojärjestelmää ja sen palveluita käytetään esimerkiksi viraston, oppilaitoksen tai työpaikan ulkopuolelta. [3, s. 9.]

2.1 Microsoftin Remote Desktop protokolla (RDP)

Microsoftin Remote Desktop -protokolla pohjautuu ja on jatke ITU T.120 -sarjan protokollaperheelle. RDP mahdollistaa etäyhteyden, jolla voidaan hallita etäkonetta ja sen syöttö- ja tulostuslaitteita, kuten näyttöä, näppäimistöä, hiirtä, sekä jakaa tiedostoja ja muita resursseja. Protokolla on suunniteltu tukemaan useita LAN-protokollia ja erilaisia verkkotopologioita. RDP tukee useita menetelmiä, joilla vähennetään verkon yli lähetetyn datan määrää, esimerkiksi tiedon pakkaus ja kuvatiedostojen siirto välimuistiin parantavat etäyhteyden suorituskykyä ja vapauttavat tiedonsiirtokapasiteettia. Käyttäjä voi siirtää, kopioida, tallentaa ja poistaa tiedostoja etäyhteyden välityksellä paikallisen ja etäkoneen välillä. Remote desktop -istunnossa kaikki ympäristömuuttujat, kuten esimerkiksi taustakuvaan ja väreihin liittyvät asetukset, määritetään RCP-TCP-yhteysasetuksista. [4.]

Yhteyden muodostus ja käsittely

Yhteydenmuodostuksen tavoitteena on vaihtaa asetuksia palvelinkoneen ja asiakaskoneen välillä sekä määrittää yhteiset asetukset etäkäyttöyhteyden ajaksi. Tämä mahdollistaa grafiikan, syöttötietojen ja muun datan vaihdon koneiden välillä. Yhteyden muodostus voidaan purkaa kahdeksaan erilliseen vaiheeseen, joissa määritetään yhteyden asetuksia. [5, s. 20–23.]

RDP:n yhteydenmuodostussekvenssi ei sisällä mitään mekanismia tai menetelmää, jolla voitaisiin varmistua palvelimen tunnistuksesta, tästä johtuen se on haavoittuva mies välissä (man-in-the-middle) -hyökkäyksille. Parannetun turvallisuuden yhteyssekvenssillä voidaan olemassa olevia turvaprotokollia, kuten TSL ja CredSSP, käyttää laajentamaan RDP:n turvallisuutta. Parannetun turvallisuuden yhteyssekvenssistä on olemassa kaksi eri variaatiota, neuvotteluperusteinen (negotiation-based) ja suora (direct) lähestymistapa. Neuvotteluperusteisessa lähestymistavassa asiakaskone ilmoittaa tukemansa turvallisuuspaketit, joista palvelinkone valitsee käytettävän menetelmän, jonka jälkeen vaihdetaan käytetyn turvallisuusmenetelmän kättelyviestit. Tästä eteenpäin RDP -liikenne on salattu valitun turvamenetelmän protokollan mukaisesti. Suora lähestymistapa poikkeaa neuvotteluperusteisesta lähestymistavasta siten, että suoritetaan suoraan ennalta määritetty turvaprotokolla, jonka johdosta koko RDP -liikenne on salattu alusta lähtien. [5, s. 24.]

Yhteydenmuodostussekvenssin päätyttyä palvelin voi päättää asiakkaan yhdistämisestä jo olemassa olevaan istuntoon. Käyttäjä voi katkaista RDP -yhteyden sulkemalla asiakassovelluksen. Asiakas lähettää palvelimelle yhteydenkatkaisupyynnön. Palvelimen vastaus riippuu siitä, onko istunto yhdistettävissä kirjautuneeseen asiakastiliin. Jos asiakastili on yhdistettävissä istuntoon, yhteyden katkaisu evätään, mutta jos asiakastiliä ei voida yhdistää istuntoon, yhteys katkaistaan välittömästi palvelimen saatua yhteydenkatkaisupyynnön. Järjestelmänvalvoja tai palvelin voi myös pakottaa käyttäjän kirjautumaan ulos tai katkaista istunnon ilman käyttäjän hallintaa. Automaattinen uudelleenyhdistys mahdollistaa asiakkaan liittymisen olemassa olevaan istuntoon, esimerkiksi lyhyestä verkkoyhteyden katkeamisesta johtuen. Palvelin voi lähettää asiakkaalle yksilöityjä virheilmoituksia ja tilapäivityksiä, jos asiakaskone tukee kyseistä menettelyä. Virheilmoituksia voidaan lähettää, jos etäyhteyden muodostaminen epäonnistuu tai asiakas on katkaisemassa yhteyttä. Tilapäivitysten avulla voidaan käyttäjälle ilmoittaa esimerkiksi aikaa vievistä prosesseista. [5, s. 24–26.]

Staattiset virtuaalikanavat (Static Virtual Channels)

Staattiset virtuaalikanavat mahdollistavat häviämättömän yhteyden RDP:tä käyttäen palvelimen ja asiakkaan välillä. Maksimissaan 31 virtuaalikanavaa voidaan luoda yhteyden aikana. Virtuaalikanavan data on riippuvaista sovelluksesta ja läpinäkyvää RDP:lle. [5, s. 26.]

Halutuista virtuaalikanavista muodostetaan lista, joka pyydetään ja varmistetaan yhteyden muodostuksen perusasetusten vaihdossa. Lisäksi päätepisteet yhdistetään kanavan yhdistysvaiheessa. Kun päätepisteet on yhdistetty, tietoa ei vaihdeta palvelimen ja asiakkaan päätepisteiden välillä vasta kun yhteydenmuodostus on päättynyt. [5, s. 26–27.]

Datan pakkaaminen

RDP käyttää massapakkaamista virtuaalikanavan datan kompressointiin sekä joidenkin datapakettien pakkaamiseen, jotka liikkuvat palvelimen ja asiakkaan välillä. Massapakkaamista käytetään tavallisen datan pakkaamisen lisäksi myös bittikarttojen pakkaamiseen, joka toteutetaan käyttäen muunnelmia jakson pituuden koodauksesta eli RLE:stä. Jakson pituuden koodaus perustuu siihen, että syötteessä peräkkäin toistuvat samat merkit korvataan erityyppisillä laskureilla, jotka kertovat, kuinka monta kertaa tietty merkki toistuu. [5, s. 26.]

Näppäimistön ja hiiren käsittely

Asiakkaalta palvelimelle menevä näppäimistö- ja hiiridata muutetaan tiedonsiirron aikana sellaiseen muotoon, jota palvelin voi parhaiten käyttää. [5, s. 27.]

Palvelimen perustulostus

Olennaisimpia tulostuksia, joita palvelin voi lähettää asiakkaalle, ovat bittikarttakuvat käyttäjän istunnosta. Tämä mahdollistaa käyttäjän vuorovaikutuksen palvelimella tapahtuvan istunnon kanssa sekä asiakkaan työskentelytilan hahmottamisen. Asiakas voi halutessaan hallita hiiren kursoria paikallisesti. isäksi palvelin lähettää asiakkaalle äänitietoja. [5, s. 27.]

Palvelimen graafisen tulostuksen hallinta

Palvelimeen yhdistetty asiakas, joka näyttää graafista dataa, voi joutua pyytämään palvelinta lähettämään uudelleen dataa kerätäkseen suorakulmaisia alueita istuntoruudusta tai pysäyttämään graafisen datan lähettämisen tietyksi ajaksi, esimerkiksi kun istuntoruutu on pienennettynä. [5, s. 27.]

Palvelimen uudelleenohjaus

Asiakasyhteys voidaan ohjata uudelleen tiettyyn istuntoon toisella palvelimella, joka mahdollistaa verkon kuormantasauksen. [5, s. 27.]

Turvallisuus

RDP:n perusturvallisuus tukee neljää eri tason salausta, jotka ovat Low, Client Compatible, High ja FIPS. Low eli matalan tason salauksessa kaikki asiakkaalta palvelimelle menevä data salataan asiakkaan maksimiavainvahvuudella. Client Compatible -salauksessa kaikki palvelimen ja asiakkaan välinen liikenne salataan asiakkaan maksimiavainvahvuudella. High-salauksessa kaikki liikenne salataan palvelimen maksimiavainvahvuudella. FIPS (Federal Information Processing Standard) on Yhdysvaltojen liittohallinnon toimesta kehitetty tietokonejärjestelmien käyttöön liittyvä standardi, jonka suosituksen 140-1 määrittelemiä salausmenetelmiä voidaan käyttää RDP-salauksessa. Kuvassa 1 on esitettynä neuvottelu käytetystä salausmenettelystä asiakkaan ja palvelimen välillä. [5, s. 388.]

Kuva 1. Käytetyn salausmenettelyn valinta RDP [5, s. 388].

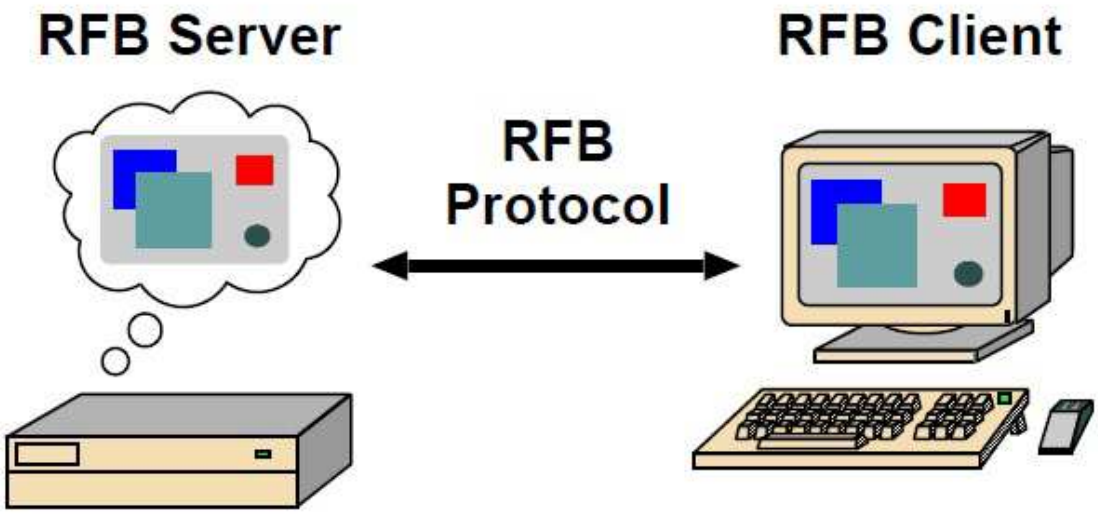
Taulukkoon 1 on koottuna edellä esiteltyjen salaustasojen ominaisuuksia. Salausmenetelmällä (Encryption Method, kuva 1) tarkoitetaan avaimen vahvuutta. Datan salauksessa nuolella (←tai→) kuvataan salauksen suunta sekä ilmoitetaan käytetty salausalgoritmi, joka on protokollan mukaisesti RC4 (luku 4.3.1). Taulukosta huomataan, että FIPS:n määrittelemä salausalgoritmi on 3DES (luku 4.3.4). Tässä dokumentissa ei kuitenkaan tarkemmin puututa FIPS:n määrittelemiin salausmenetelmiin.

Taulukko 1. RDP salaustasojen vertailu [5, s. 398].

Salaustaso	Salausmenetelmä	Datan salaus
Low	40-bit, 56-bit, 128-bit	asiakas → palvelin, RC4
Client Compatible	40-bit, 56-bit, 128-bit	asiakas ← → palvelin, RC4
High	128-bit	asiakas ← → palvelin, RC4
FIPS	FIPS	asiakas ← → palvelin, 3DES

2.2 RFB-protokolla

RFB eli Remote Framebuffer-protokolla mahdollistaa palvelimen (server) graafisen käyttöliittymän hallinnan ”etänä” asiakaskoneella (client) (kuva 2). Protokolla toimii kehyspuskuritasolla, joten se soveltuu kaikille ikkunointijärjestelmille ja sovelluksille, kuten Windowsille, X11:lle ja Macintoshille. VNC eli Virtual Network Computing-järjestelmät käyttävät RFB:tä. RFB on ”thin client” -protokolla, joka asettaa vähän vaatimuksia asiakkaalle. [6, s. 3.]



Kuva 2. RFB-protokolla [6, s. 3].

Protokollan näytölle tulostus perustuu siihen, että tietty ruutu pikselidatasta asetetaan tiettyyn kohtaan näytöllä. Erilaiset näyttödatan koodaustavat mahdollistavat joustavan tietojen vaihdon palvelimen ja asiakkaan välillä, kuten esimerkiksi palvelimen suoritusnopeuden, asiakkaan piirtonopeuden ja verkon kaistanleveyden vaihdon. Näytön päivitys tapahtuu asiakkaan

vaatimuksesta, eli palvelin vastaa ainoastaan asiakkaan pyyntöihin. Tämä mahdollistaa sopeutumisen verkon tai asiakkaan hitauteen, jolloin ruudun päivitysnopeus laskee. [6, s. 3–4.]

Protokollan syöttöosa pohjautuu perinteiseen työasemamallin mukaiseen näppäimistöön ja moninäppäimiseen osoitinlaitteeseen. Syöttötiedot lähetetään palvelimelle, kun asiakas–koneella painetaan näppäintä näppäimistöstä tai osoitinlaitteesta ja kun liikutetaan osoitinlaitetta. Syöttötapahtumia voidaan tuoda myös muista I/O-laitteista, jotka eivät ole standardin mukaisia. [6, s. 4.]

RFB-asiakkaan ja -palvelimen yhteydenmuodostusvaiheessa sovitaan pikselidatan koodauksesta ja formaatista. Koodauksella tarkoitetaan sitä, kuinka ruutu pikselidatasta syötetään siirtotielle. Ruuduille on annettu osoite(header) -kenttään X,Y –paikka, johon ruutu sijoitetaan, ruudun korkeus ja leveys sekä koodaustapa. Määritettyjä koodaustapoja ovat ”CopyRect”, ”Raw”, ”Hextile”, ”RRE” ja ”ZRLE”, joista käytännössä käytetään ainoastaan Hextileä, CopyRectiä ja ZRLE:ä. Pikselin formaatilla viitataan siihen, kuinka värit esitetään pikselitasolla. Yleisimmät pikseliformaatit ovat 24- ja 16-bittiset ”true color” -formaatit. Palvelimen täytyy aina lähettää pikselidata siinä muodossa, missä asiakas sen haluaa. Kuitenkin jos asiakas kykenee käsittelemään useita koodausmenetelmiä, se voi valita sellaisen menetelmän, joka on palvelimen helpointa tarjota.[6, s. 4–5.]

Turvallisuus

Palvelimen ja asiakkaan sovittua käytetystä protokollaversiosta asiakas valitsee käytetyn turvallisuustyypin kättelyssä palvelimen ilmoittamista vaihtoehdoista (versiosta 3.7 eteenpäin) tai palvelin ilmoittaa käytettävän turvallisuusmenettelyn (versio 3.3) [6, s. 9–10]. Protokolla tukee useita turvallisuusmenettelyjä, mutta dokumentissa määritetyt ovat Invalid, None ja VNC Authentication.

Käytännössä Invalid tarkoittaa yhteyden epäonnistumista ja None ilman mitään turvakäytäntöä muodostettua yhteyttä eli kaikki data lähetetään salaamattomana yhteyden osapuolten välillä. VNC Authenticationissa eli tunnistuksessa käytetään haaste-vastaus-menetelmää, jossa palvelin lähettää asiakkaalle 16-tavuisen haasteen. Asiakas purkaa haasteen DES:llä käyttäen annettua salasanaa ja lähettää palvelimelle 16-tavuisen vastauksen. Käytettäessä VNC Authenticationia, varsinainen data lähetetään tunnistuksen jälkeen salaamattomana. [6, s. 14.]

3 LÄHIVERKKO

Etäkäyttöympäristö on toteutettu lähiverkkoympäristössä, joista yleisimmin käytetty tekniikka on Ethernet-verkko, joka on määritetty IEEE 802.3 -sarjan suosituksissa. Tässä luvussa esitellään taustaa lähiverkoista sekä sitä, minkälaisilla laitteilla verkkoja toteutetaan.

3.1 OSI-malli

OSI-malli esittää, kuinka tietojärjestelmiä voidaan liittää toisiinsa. Arkkitehtuurin perustana on kerrosmalli, jossa tarjotaan palveluita ylemmälle kerrokselle ja käytetään hyväksi alemman kerroksen palveluja. Kerrosarkkitehtuuri on esitetty ISO 7498 -suosituksessa. [7, s. 6.]

Fyysinen kerros määrittää yhteyden fyysiset, toiminnalliset ja mekaaniset osat sekä prosessin, jossa bitit muutetaan siirtomedialle sopivaan muotoon. Siirtoyhteyskerros on käytännössä jakautunut kahteen osaan: MAC ja LLC. MAC-kerros varaa siirtoyhteyden. LLC-kerros havaitsee ja toipuu virheistä fyysisellä kerroksella sekä hallitsee tietovuota. Verkkokerros muodostaa yhteyden ottamatta kantaa kytkentätekniikkaan tai verkon rakenteeseen. Käytännössä verkkokerros huolehtii reitityksestä eli pyrkii löytämään optimaalisen reitin lähettäjältä vastaanottajalle. Verkkokerros muuttaa laitteiden loogiset osoitteet fyysisiksi osoitteiksi ja nimet loogisiksi osoitteiksi sekä sovittaa sanoman siirtotielle sopivaan muotoon niin sanotuiksi paketeiksi. [7, s. 8–10.]

Kuljetuskerros tarjoaa joko yhteydettömän tai yhteydellisen yhteyden päätepisteiden välille. Yhteydettömässä yhteydessä sanoma lähetetään ilman yhteyden muodostusta vastaanottajalle, eikä sanoman perille pääsyä valvota. Yhteydellisessä yhteydessä yhteys luodaan joka kerta ja sanoman lähetystä seurataan, jotta esimerkiksi lähetetyt paketit saapuvat oikeassa järjestyksessä. Istuntokerroksen tehtäviin kuuluu huolehtiminen sovellusten välisestä ohjaustoiminnasta eli yhteyden muodostuksesta, yhteyden ominaisuuksista sopimisesta osapuolten välillä, siirtoyhteyspalvelun varaamisesta, yhteyden varmistamisesta, yhteyden päättämisestä ja resurssien vapauttamisesta yhteyden päättämisen jälkeen. Esitystapakerroksen tehtävänä on sopia yhteisestä tiedon esitystavasta lähettäjän ja vastaanottajan välillä. OSI-mallissa sovelluskerroksen tehtävänä on tarjota rajapinta sovelluksille, esimerkiksi sähköpostille. [7, s. 8–10.]

Kuvassa 3 on esitettynä OSI-mallin kerrokset.

Kuva 3. OSI-malli

3.2 TCP/IP -viitemalli

TCP/IP -protokollaperheen protokollat määrittävät sanomaliikennettä ja sovellusten toimintaa pääosin silloin kun sovelluksen palvelin- ja asiakasosa ovat eri verkoissa [8, s. 398]. Periaatteessa TCP/IP:tä voidaan OSI-mallin tapaan pitää kerrosarkkitehtuurina, vaikkakaan se ei sitä varsinaisesti ole. TCP/IP:n kerrokset ovat liittymäkerros, internet-kerros (verkkoprotokollat), kuljetuskerros ja sovelluskerros. Liittymäkerros kattaa OSI-mallin kaksi alinta kerrosta, eli ”kerros” vastaa käytännössä laitteen liittämisestä verkkoon. Internet-kerroksen tehtävänä on siirtää sanomia verkon yli yhteydettömällä yhteydellä, eli sopimusta yhteyden muodostuksesta osapuolten välillä ei ole. Internet-kerroksen protokollia ovat IP, ICMP ja IGMP. IP välittää ylempien protokollatasojen tiedot verkkokorttiajurille. ICMP:tä käytetään verkon laitteiden hallintaviestien lähettämiseen, ja IGMP:n käyttötarkoitus on multicast-ryhmien hallinta. Kuljetuskerrokset OSI-mallissa ja TCP/IP:ssä muistuttavat toimintaperiaatteeltaan toisiaan. Kuljetuskerroksen tehtäviin kuuluu muun muassa vuonhallinta ja datan pilkkominen sopiviin osiin alemman tason protokollille, kuten IP:lle. TCP/IP:n kuljetuskerroksen protokollat ovat UDP ja TCP, joista UDP on yhteydetön ja TCP yhteydellinen, eli TCP:ssä yhteyden muodostuksesta ja sen ominaisuuksista sovitaan asiakkaan ja palvelimen välillä. Sovellustasolla on iso joukko erilaisia protokollia, jotka lähettävät tietoa asiakkaan ja palvelimen välil-

lä, esimerkkinä HTTP, jota käytetään selainten ja WWW-palvelimien tiedonsiirtoon. [8, s. 398–401.][7, s. 6–7.]

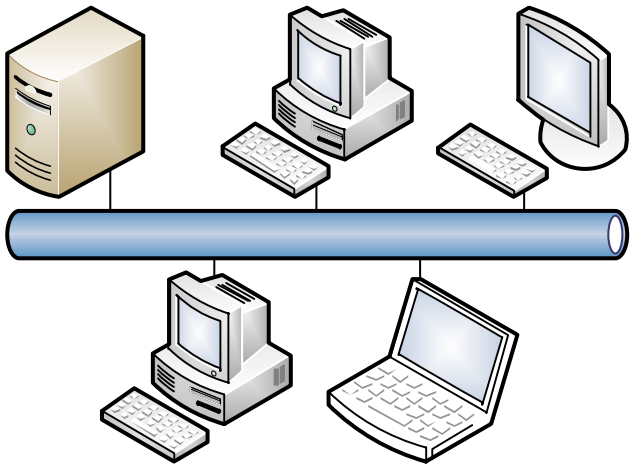
Kuvassa 4 on esitettynä TCP/IP -viitemallin kerrokset ja kerrosten tasolla toimivat protokollat.

TCP/IP -kerrokset	Protokollat
SOVELLUSKERROS	Sovellukset (http, FTP ja niin edelleen.)
KULJETUSKERROS	Kuljetusprotokollat (TCP ja UDP)
INTERNET-KERROS	Verkkoprotokollat (ICMP,IP ja IGMP)
LIITTYMÄKERROS	Verkkokorttit (-ajurit)

Kuva 4. TCP/IP -viitemallin kerrokset ja vastaavat protokollat.

3.3 IEEE 802.3

IEEE 802.3 -sarjan suositukset määrittävät Ethernet-verkkoja, joka on yleisin lähiverkkotyyppi. Verkkotopologialtaan Ethernet on väylä tai tähti, mutta kanavanvarauksen perusteella puhutaan väylästä, jonka kilpavarausta törmäyksentunnistuksella kuvataan IEEE 802.3 -suosituksissa (kuva 5). Suosituksen toiminta perustuu siihen, että kaikki verkkoon kytketyt laitteet tarkkailevat verkon tilaa. Jos laite havaitsee, ettei väylällä ole liikennettä, se lähettää oman sanomansa eli puhutaan niin sanotusta vuorosuuntaisesta liikenteestä. Jos laite havaitsee törmäyksen väylällä tai jokin muu on aloittanut lähettämisen yhtä aikaa, laite odottaa tietyn ajan ennen kuin lähettää datan uudelleen. [9, s. 240.] [7, s. 262.]



Kuva 5. Ethernet-verkko

IEEE 802.3x -suositus määrittää kaksisuuntaista eli full duplex-liikennettä kahden verkkolaitteen välillä. Se sisältää muun muassa vuonhallintamekanismin, jolla vastaanottaja voi pysäyttää lyhyeksi aikaa lähettäjältä tulevan liikenteen. Yhteysmuoto on mahdollista vain kaksipisteyhteyksillä (point-to-point). Ethernet-verkon nykyiset laitteet osaavat optimoida kaksipisteyhteydelle sopivat ominaisuudet, jotta tiedonsiirtolinjaa käytetään parhaalla mahdollisella tavalla. Tästä käytetään nimitystä auto-negotiation. Auto-negotiation on toteutettu laitetasolla, mutta sen tilaa voidaan hallita käyttäjän toimesta tai estää tietyn ominaisuuden toiminta. Edellytyksenä kuvatulle menetelmän käytölle on se, että yhteyden molemmat osapuolet hallitsevat menetelmän ja kykenevät käyttämään sitä. [7, s. 275–276.]

Parikaapeliyhteyksiä käyttävä Ethernet verkko eli 10Base-T esiteltiin suosituksessa IEEE 802.3i vuonna 1990. Jatkossa kehitettiin 100Base-Ethernet eli Fast Ethernet, joka on määritetty suosituksessa 802.3u ja jonka nopeus on 100 Mbit/s. Suositus 802.3z, joka esiteltiin vuonna 1998, määrittää Gigabit Ethernetin, jonka nopeus on 1000 Mbit/s. Nopeudella 10 Gbit/s toimiva Ethernet-verkko on esitelty suosituksessa IEEE 802.3ae. [7, s. 262–263.]

3.4 Verkon aktiivilaitteet

Verkon aktiivilaitteita ovat verkkokortti, toistin eli hub, kytkin, silta ja reititin.

Verkkokortin tehtävänä on luoda yhteys tietokoneen lähiverkon välille. Verkkokortteja on useita erityyppisiä ja jaottelutapana käytetään esimerkiksi sitä, mihin tietokoneväylään verkkokortti kytketään. Nykyisin yleisesti käytetään PCI-, PCI Express- ja PCMCIA -väyliin liitettäviä kortteja. Verkkokortista käytetään myös nimitystä NIC eli Network Interface Card. Valmistaja on antanut jokaiselle verkkokortille oman 48-bittisen MAC-osoitteen, jonka perusteella verkkokortti on yksilöitävissä. [9, s. 233.][10, s. 114–123.]

Toistinta käytetään esimerkiksi verkon jatkamiseksi, koska se vahvistaa signaaleja ja tarvittaessa korjaa ajastusta sekä toistaa signaalit eteenpäin. Toistin toimii OSI-mallin fyysisellä kerroksella(1), päästäen lävitseen kaiken liikenteen, tutkimatta datan sisältöä tai MAC-osoitteita. Parikaapeliverkon toistimista käytetään nimitystä hub tai keskitin. Hub on käytännössä moniporttitoistin, eli yhteen porttiin tuleva data toistetaan kaikille muillekin porteille. [11.]

Silta suodattaa liikennettä MAC-osoitteiden perusteella ja tarvittaessa jatkaa verkkoa. Siltaa käytetään yhdistämään samanlaiset verkot tai erottelemaan liikennettä esimerkiksi kuormituksellisista syistä. Riippuen toimintaympäristöstä, sillat voidaan jakaa etäsiltoihin ja paikallissiltoihin. Etäsilta yhdistää fyysisesti kaukana toisistaan sijaitsevia verkkoja ja paikallissilta yhdistää kaksi viereistä lähiverkkoa. Sillat oppivat liikennettä tarkkailemalla laitteiden sijainnit, eivätkä verkon muut laitteet tiedä sillan olemassaolosta. Silta toimii OSI-mallin siirtokerroksella. Siltojen käyttö on vähentynyt voimakkaasti, koska kytkimet ovat pääosin korvanneet sillat. [11.]

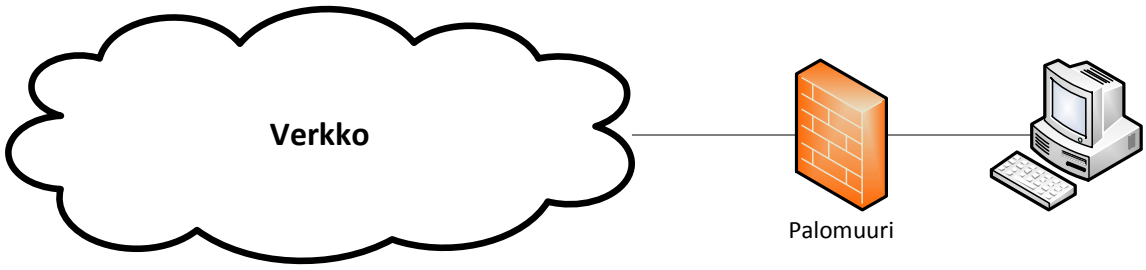
Kytkin on käytännössä moniporttinen silta. Nykyisin lähiverkkojen rakentamisessa käytetään pääosin kytkimiä. Kytkin välittää samanaikaisesti useita eri porttien välisiä yhteyksiä. Tämä kasvattaa tiedonsiirtokapasiteettiä verrattuna keskittimillä toteutettuihin verkkoihin. Kytkimiä voidaan hallita ja muokata käyttäjän toimesta eli määrittää esimerkiksi virtuaaliverkkoja. Kytkimet toimivat yleisesti OSI-mallin 2-tasolla, jolloin kytkentä tapahtuu MAC-osoitteiden perusteella, mutta olemassa on myös tason 3 eli verkkotason kytkimiä, jotka suorittavat reitityksen IP-osoitteiden perusteella. Sovelluskytkimillä kytkentä tapahtuu sovellusprotokollan perusteella. [11.]

Reitittimet yhdistävät ja erottavat verkkoja. Verrattuna kytkimiin reitittimet ovat paljon kehittyneempiä. Niillä voidaan määrittää muun muassa, kenellä on oikeus liikennöidä ja minne, sekä ohjata verkkojen välistä liikennettä. Reititin ohjaa paketit vastaanottajalle verkko-osoitteen perusteella. Reititin käyttää saapuvan paketin IP-osoitteen aliverkon peitettä päätelläkseen kohdeosoitteen verkko-osan. Tästä reititin tietää, minne paketti tulee ohjata. Reitittimet ylläpitävät reititystauluja, joita reitittimet vaihtavat keskenään perustuen tiettyihin protokolliin. Reitittimillä on kattava kuvaus verkosta, ja ne kykenevät käyttämään kaikkia verkkoja samanaikaisesti sekä optimoimaan käytettävän reitin. Reititin on myös hallittava laite, jolle määritetään käytettävät reititysprotokollat, pääsylistat ja porttien käyttö. Reitittimet toimivat OSI-mallin verkkokerroksella. Reitittimet pystyvät suodattamaan liikennettä esimerkiksi lähetysprotokollan, lähettäjän, sanomatyypin, vastaanottajan ja sen perusteella, mistä aliverkosta sanoma on lähetetty[9, s. 236]. [11.]

3.5 Palomuuri

Palomuurilla tarkoitetaan yleisesti laitetta tai ohjelmistoa, jolla estetään asiattomien henkilöiden pääsy verkkoon tai verkon palveluihin. Yleisimmin palomuurit toimivat lähiverkon ja julkisen verkon rajalla, tarkkaillen ja suodattaen verkkoliikennettä. Palomuuri tulisikin sijoittaa siten verkon rajalle, että kaikki verkkoliikenne kulkee sen kautta. Palomuurit voidaan jaotella toimintatapansa perusteella välityspalvelimiin, pakettisuodattimiin ja sovellustason yhdyskäytäviin. Välityspalvelimet avaavat yhteyden tiettyyn palveluun, kun on määritelty laite, jolle yhteys sallitaan. Välityspalvelimet mahdollistavat myös käyttäjän tunnistuksen ennen yhteyden avaamista. Välityspalvelimien ongelmana pidetään sitä, että yhteys on avoin, kunnes palvelin sen sulkee. Pakettisuodattimien toiminta perustuu siihen, että ne hylkäävät ja sallivat liikennettä tiettyjen sovellusten käyttämien porttien perusteella, sekä joihinkin lähde- ja kohdeosoitteisiin. Sovellustason yhdyskäytävä välittää liikennettä palvelin- ja asiakasohjelmiston välillä, tutkien jokaisen paketin sisällön. Havaitessaan epätavallisen paketin sovellustason yhdyskäytävä tekee hälytyksen ylläpitäjälle ja tallentaa tarvittaessa tämän paketin myöhempää tarkastelua varten. [8, s. 187–188.]

Kuvassa 6 on esitetty periaatteellinen kuva palomuurin toiminnasta.



Kuva 6. Palomuurin pelkistetty toiminta.

3.6 Kaapelointi

Lähiverkkojen kaapeloinnissa käytetään yleisesti parikierrettyä kaapelia, joka pohjautuu puhelinverkkoihin. Parikaapelijohtimet jaotellaan Cat-kategorioihin. Luokittelu on esitetty taulukossa 2.

Taulukko 2. CAT-kategoriat [9, s. 42–45].

CAT -kategoria	**Kaistanleveys, MHz:iä**	**Kuvaus**
1 ja 2	-	Kyseiset luokat eivät ole nykyisin juurikaan käytössä.
3	16	Kuvattu EIA/TIA-586 -suosituksessa. Käyttökohteena 10Base-T-verkot.
4	20	Käytetään järjestelmissä joissa tiedonsiirtonopeus on enintään 20 Mbit/s. Esimerkkinä Token Ring.
5	100	Enintään 100 Mbit/s -tiedonsiirtojärjestelmien, kuten 100Base-TX ja 1000Base-T toteutukseen.
5e	100	Parannettu versio Cat-5:stä. Testausstandardeja tiukennettu.
5E	250	Ei ole standardoitu.
6, 6a, 6e	250, 250, 500	Pohjautuu TIA/EIA-568-B.2-1 -suositukseen. Cat-6 käytetään 1000Base-T- ja Cat-6a 10GBase-T-järjestelmissä.
7	600	Käyttää omaa GG45-liitintä ja S/STP-kaapelia. Käytetään 10Gb-Ethernet -verkoissa.

Parikaapelit voidaan jaotella myös sen perusteella, ovatko ne suojaamattomia eli UTP tai suojattuja eli STP. Parikaapeloinnissa käytetään yleensä kahdeksanpinnistä RJ45–liitintä. [9, s. 44–45.]

Ethernet-verkkojen fyysisiä tasoja kuvataan siten, että ensimmäisenä ilmoitetaan nimellisnopeus, seuraavana base(band) eli kantaajuus tai broad(band) eli laajakaista, ja lopuksi kaapelointikoodi. Esimerkiksi 10Base-T tarkoittaa 10 Mbit/s kantataajuusperiaatetta käyttävää parikaapeliyhteyttä. [9, s. 280–289.]

4 ETÄKÄYTÖN TIETOTURVALLISUUS

Etäkäytössä tulee ottaa huomioon myös tietoturva. Tässä luvussa käsitellään peruskäsitteistöä, salausjärjestelmiä (-algoritmeja), salausprotokollia ja pintapuolisesti myös salattuja etäyhteyksiä.

4.1 Tietoturvan määrittely

Tietoturvallisuudelle tai tietoturvalla on olemassa standardista tai lähteestä riippuen erilaisia määritelmiä, mutta kaikkien yhteisenä ominaisuutena voidaan pitää tietoa, joka on nopeasti saatavilla, oikeiden henkilöiden ulottuvilla, luotettavaa, sekä tieto on oikeassa muodossa. Tiedon käsitteestä liikkeelle lähteneeseen määritelmään on sisällytetty usein tiedon käsittelyssä käytetyt laitteistot ja järjestelmät. Toinen tapa laajentaa tietoturvan määritelmää on juridinen, jolloin järjestelmän tulee kertoa, kuka tiedon on luonut. Sillä kuka tiedon ”omistaa” tai on siitä vastuussa, on suuri merkitys erityisesti sähköisessä kaupankäynnissä ja muissa sähköisessä asioinnin menetelmissä. [8, s. 4.]

Klassisessa tiedon arvoon pohjautuvassa määritelmässä tietoturvallisuuden kolme osatekijää ovat käytettävyys, luottamuksellisuus ja eheys. Käytettävyydellä tarkoitetaan sitä, että tieto on saatavilla järjestelmässä riittävän nopeasti sekä oikeassa muodossa. Luottamuksellisuudella tarkoitetaan sitä, että tietoa pääsevät tarkastelemaan vain siihen oikeutetut henkilöt. Eheys voidaan määritellä siten, että järjestelmän tiedot ovat paikkansa pitäviä ja eivät sisällä virheitä (tahallisia tai tahattomia). Klassista määritelmää pidetään nykyisin usein riittämättömänä. Tästä johtuen sitä on laajennettu kahdella uudella osatekijällä, jotka ovat pääsynvalvonta ja kiistämättömyys. Lisäksi joissakin tapauksissa määritelmän on otettu vielä kuudes tekijä, joka on autenttisuus. Pääsynvalvonnalla tarkoitetaan keinoja, joilla rajoitetaan tietojenkäsittelyjärjestelmien käyttöä. Pääsynvalvontaa ei pidä sekoittaa luottamuksellisuuden käsitteeseen, koska luottamuksellisuuden ylläpidon menetelmillä rajoitetaan ainoastaan varsinaisiin tietoihin pääsyä. Kiistämättömyydellä tarkoitetaan tilannetta, jossa järjestelmä tunnistaa sekä tallentaa käyttäjän tiedot luotettavasti. Kiistämättömyyden tavoitteena on varmistaa tiedon alkuperä tai tunnistaa tilanne, jossa tietoja käytetään luvattomasti. Autenttisuudella pyritään tunnistamaan järjestelmän käyttäjä tai käytetty laite. Koska käyttäjän tunnistus on edellytys sekä kiis-

tämättömyydelle että luottamuksellisuudelle, se jätetään yleensä pois tietoturvallisuuden määritelmästä. [8, s. 4–6.]

4.2 Uhkakuvat ja riskit etähallintaan liittyen

Etäkäytölle ja etätyöpöytäyhteyksille on olemassa omat riskinsä ja uhkakuvansa, joista tässä esitellään muutamia.

4.2.1 Man in the Middle -hyökkäykset

Jos hyökkääjä pystyy väärentämään verkon reititystaulukon ja lähettämään väärennettyjä viestejä, hän voi tehdä man-in-the-middle- eli suomeksi mies välissä -hyökkäyksen. Kun tunkeutuja on väärentänyt reititystaulukon, hän ohjaa kahden tietokoneen välisen liikenteen kokonaisuudessaan kulkemaan hyökkääjän tietokoneen kautta. Tunkeutuja pystyy näin ollen tarkkailemaan kaikkea liikennettä yhteyden osapuolten välillä. Jos yhteydenmuodostuksessa käytetään jotakin istuntoavainta, tunkeutuja sopii molemmille laitteille eri avaimet. Näin hän voi purkaa viestit jokaisessa vaiheessa ja lähettää viestit edelleen mahdollisesti muokattuna, käyttäen toisen osapuolen kanssa sovittua avainta. Keskenään viestivät tietokoneet eivät huomaa yhteyden välissä olevaa tunkeutujaa. [12, s. 338–339.]

4.2.2 Ohjelmistojen haavoittuvuudet

Symantec-yhtiön etäkäyttöohjelmistossa pcAnywhere havaittiin alkuvuodesta 2012 kaksi haavoittuvuutta, joista toinen mahdollisti käyttövaltuuksien korotuksen paikallisesti kirjautuneelle käyttäjälle ja toinen haavoittuvuus mahdollisti hyökkääjän suorittaa omaa ohjelmakoodia kohdejärjestelmässä, mikä johtui käyttäjäntodennuksen syötteentarkistuksen puutteista. Haavoittuvuudet korjattiin ohjelmistopäivityksellä. Lisäksi suositeltiin verkkoliikenteen rajoituksia ohjelmiston käyttämään TCP-porttiin 5631. [13.]

Elokuussa 2011 varoitettiin Morto-haittaohjelmasta, joka etsii verkosta koneita, jotka käyttävät Windowsin etätyöpöytäpalvelua. Haittaohjelma lähettää RDP-yhteyspyynnön, ja jos jokin kone vastaa pyyntöön, haittaohjelma pyrkii kirjautumaan koneeseen järjestelmänvalvojana. Kirjautumisessa käytetään hyväksi yleisesti tunnettuja heikkoja salasanoja. Kyseiseltä haittaohjelmalta voidaan suojautua käyttämällä riittävän vahvoja järjestelmänvalvojan salasanoja sekä mahdollisesti rajoittamalla liikennettä RDP-protokollan käyttämään TCP-porttiin 3389. [14.]

4.3 Salausmenetelmät

Salausmenetelmien käytön tarkoituksena on varmistaa tietojen eheys, luottamuksellisuus ja kiistämättömyys. Käyttötarkoituksesta riippumatta salauksen tulisi olla riittävän vahva, jotta sen murtaminen ei olisi mahdollista kohtuullisessa ajassa ja tietyillä resursseilla. Kohtuullisen ajan ja resurssien määritelmä riippuu salattavan tiedon tärkeydestä. Vahvoilla salausmenetelmillä tarkoitetaan sellaisia menetelmiä, joiden murtaminen saatavilla välineillä ei ole mahdollista. Vahvoja salausmenetelmiä voidaan käyttää nykyisin laajasti, johtuen tietokoneiden suuresta laskentakapasiteetista. Suomessa salauksen tasoa ei ole rajoitettu lainsäädännössä, kuten monissa muissa valtioissa. [15.]

Salausmenetelmien turvallisuuden perustana ovat salausavaimet, ja salausmekanismin julkisuus tai salaisuus ei vaikuta turvallisuuteen. Kun järjestelmä on toteutettu hyvin, salaus voidaan purkaa ainoastaan käymällä läpi kaikki salausavaimet avainavaruudesta. Salauksen vahvuuden mittaamisessa tai arvioinnissa voidaan käyttää avaimen pituutta, eli mitä pidempi salausavain, sitä vahvempi salaus on kyseessä. Salausmenetelmät voidaan jakaa kahteen luokkaan, lohkosalaukseen ja jonosalaukseen. Jonosalaajia käytetään nopeissa reaaliaikasovelluksissa, yleensä salaamalla tietoa merkki kerrallaan. Lohkosalauksen toimintaperiaatteena on tiedon salaaminen lohko kerrallaan. Lohkosalausta käytetään symmetrisissä ja epäsymmetrisissä salausalgoritmeissa.[15.]

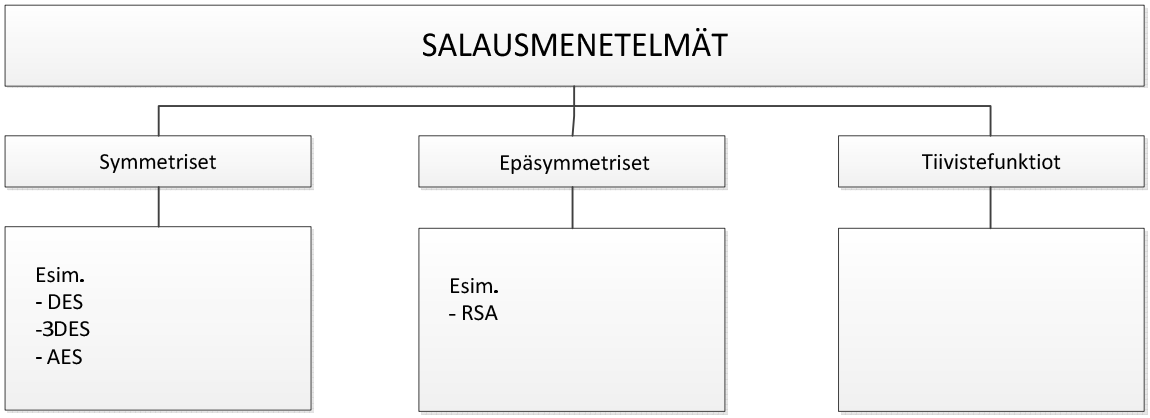
Salausmenetelmien luokittelussa voidaan käyttää myös menetelmää, jossa luokittelu tapahtuu sen perusteella, miten selväkielisiä sanomia käsitellään. Korvaussalaajat salaavat sanoman lohko kerrallaan korvaamalla selväkielisen lohkon salasanoman lohkolla. Korvaussalaajan salasanoman lohko muodostuu salausalgoritmista ja -avaimesta, joka voidaan vaihtaa missä vaiheessa tahansa. Siirtosalaajat muodostavat salatun lohkon käyttäen aina samaa algoritmia.

Tulosalaajat salaavat lohkot käyttämällä useita eri salakirjoitusmenetelmiä. Sekoitussalaajat järjestävät uudelleen salattavan lohkon sisällön salausavaimen ja salausalgoritmin velvoittamalla tavalla. [8, s. 374–375.]

Symmetrisissä salausalgoritmeissa salauksessa ja salauksen purussa käytetään samaa avainta. Epäsymmetrisissä algoritmeissa eli julkisen avaimen algoritmeissa käytetään eri avaimia sanoman salaukseen ja purkuun. Symmetristen menetelmien etuna on nopeus, mutta avainten hallinta voi olla ongelmallista, sillä sekä viestin lähettäjän että vastaanottajan tulee tietää käytetty avain. Avainten turvallinen jakaminen käyttäjien välillä on tärkeää. Epäsymmetriset menetelmät ovat hitaita, mutta julkisten avainten vapaa jakelu on etuna verrattuna symmetrisiin järjestelmiin. Epäsymmetrisessä salauksessa käytetään niin sanottua kahden avaimen menetelmää eli julkista (public) ja yksityistä (private) avainta. Kun viesti on salattu käyttäen vastaanottajan julkista avainta, vastaanottaja purkaa salauksen käyttäen omaa yksityistä avaintaan. Jos vastaanottajan yksityistä avainta ei tiedetä, tunkeutuja ei voi avata viestiä, joka on salattu julkisella avaimella. Monet salausjärjestelmät käyttävät hyväkseen molempia algoritmityyppejä, eli epäsymmetristä salausta käytetään yhteyden muodostuksen aikana symmetrisen avaimen sopimiseksi ja tällä symmetrisellä avaimella toteutetaan varsinainen salaus. [15.]

Tiivistefunktioita, joita käytetään digitaaliseen allekirjoitukseen ja salasanojen tallennukseen, muodostetaan siten, että pitkästä syötteestä lasketaan lyhyt määrämittainen tiiviste. Tiivistefunktiot ovat funktioita, joiden vastauksesta on hankala muodostaa lähtöarvoa [8, s. 373–374]. Digitaalisen allekirjoituksen toimintaperiaatteena on tiivisteiden vertailu, eli lähettäjä muodostaa viestistä tiivisteen, jonka hän lähettää vastaanottajalle yleensä salattuna, jonka jälkeen vastaanottaja laskee myös viestistä tiivisteen. Jos tiivisteet ovat samat, viestiä ei ole muutettu. Tiivistefunktioista käytetään myös nimityksiä hajautusfunktiot tai yksisuuntaiset funktiot. [15.]

Kuvassa 7 on esitetty salausmenetelmien jako symmetrisiin, epäsymmetrisiin ja tiivistefunktioihin.



Kuva 7. Salausmenetelmien jako.

4.3.1 RC4

RC4 on yksinkertainen symmetrinen jonosalaaja, joka salaa tiedon tavu kerrallaan ja perustuu satunnaiseen permutaatioon. RC4 käyttää vaihtuvaa avainpituutta, ja se koostuu kahdesta algoritmista KSA ja PRGA. RC4 suunniteltiin vuonna 1987 Ron Rivestin toimesta RSA Security-yhtiölle ja se on yleisimpiä käytettyjä jonosalaajia. RC4:ää käytetään esimerkiksi SSL:ssä ja TLS:ssä. Käytännössä salaus tapahtuu siten, että KSA:sta ja PRGA:sta muodostetaan niin sanottu avainvirta (keystream), joka yhdistetään XOR-operaatiolla tavu kerrallaan salattavaan sanomaan. [16, s. 192–196.]

Esimerkiksi jos salattava sanoma on binäärimuodossa 10101110 ja sen hetkinen avainvirran arvo on 00110101, saadaan XOR-operaatiolla salatuksi sanomaksi 10011011.[16, s. 192–193.]

Kuten yllä olevasta huomataan, kriittinen tekijä kyseisessä salausmenetelmässä on saman satunnaisluvun muodostus molemmissa vaiheissa, eli salauksessa ja salauksen purussa.

4.3.2 AES

Advanced Encryption Standard on kehitetty Yhdysvaltain hallituksen toimesta korvaamaan DES-algoritmi. AES:n toiminta perustuu niin sanottuun Rijndael-algoritmiin, joka on salaisen avaimen tulosalaaja ja jota voidaan käyttää myös tiivistefunktiona. Rijndael-algoritmi käyttää joko 128- , 192- tai 256-bittistä avain, lisäksi salattavan lohkon koko on 128, 192 tai 256 bittiä. [8, s. 382.][16, s. 143–145.]

Jokainen sanoma ja salakirjoitusavain järjestetään omiin taulukoihinsa. Taulukoissa on neljä riviä. Sarakkeiden määrä saadaan laskettua jakamalla lohkon tai avaimen pituus 32:lla (bitteinä). Taulukon täyttö tapahtuu sarake kerrallaan, käyttäen lohkon tai avaimen tavuja. Algoritmi käyttää useita salauskierroksia, joiden lukumäärä valitaan joko avaintaulukon tai lohkotaululukon sarakkeiden perusteella, siten että neljä saraketta tarkoittaa kymmentä salauskierrosta ja kuusi saraketta kahtatoista kierrosta ja niin edelleen. Seuraavassa vaiheessa avaimesta muodostetaan kierrosavaimet jokaiselle salauskierrokselle sekä lopun ylimääräiselle kierrokselle. Tämän jälkeen lohkotaulukon alkioita muutetaan käyttäen avaintaulukon alkioita, jonka jälkeen suoritetaan varsinaiset salauskierrokset. Jokaisella salauskierroksella lohkotaulukon alkiot salataan korvaussalaajalla, alkioiden sijaintia siirretään rivin sisällä riippuen taulukon sarakkeiden lukumäärästä, korvaussalaajalla salataan sarake kerrallaan ja lopuksi alkiot muutetaan kierrosavaimen perusteella. Ylimääräisellä salauskirjoituskierroksella toimitaan kuten muulloinkin, mutta sarake kerrallaan tehtävä salaus jää pois. Jokainen selväkielisen sanoman lohko salataan edellä mainitulla tavalla. [8, s. 382.][16, s.145–149.]

4.3.3 RSA

Ron Rivest, Adi Shamir ja Lend Adleman kehittivät RSA:n, joka on epäsymmetrinen julkisen avaimen salausalgoritmi. RSA:n turvallisuus perustuu olettamukseen, että kahdesta suuresta alkuluvusta muodostetun luvun jakaminen tekijöihin on vaikeaa. [17, s. 156.] [8, s. 382–383.]

RSA:n yksityisen ja julkisen avaimen muodostuksen vaiheet ovat [16, s. 270–271]:

- Valitaan kaksi suurta alkulukua p ja q, $p \neq q$.
- Lasketaan n=pq.

- Valitaan luku e, siten ettei luvulla e ja tulolla (p-1)(q-1) ole yhteisiä tekijöitä.

- Lasketaan d.

$$d = e^{-1} mod[(p-1)(q-1)]$$

Yllä olevasta saadaan julkinen avain KU={e,n} ja yksityinen avain KR={d,n}, eli vain lähettäjä tietää luvun e ja vastaanottaja luvun d, mutta molemmat tietävät luvun n, joka on julkisesti saatavilla [16, s.268]. Selväkielinen sanoma M, joka on pienempi kuin n (M<n), salataan seuraavasti:

$C = M^e (mod\ n)$, jossa C on salattu teksti

Salauksen purku takaisin selväkieliseen muotoon tapahtuu seuraavasti.

$M = C^d (mod\ n)$

4.3.4 DES

Data Encryption Standard on symmetrinen lohkosalaaja, jossa lohkon pituus on 64-bittiä ja avaimen koko 56-bittiä. Pelkkää DES-salausta ei voida nykyisin pitää turvallisena, mutta DES:stä kehitetyt algoritmit, kuten 3DES ovat edelleen käytettyjä menetelmiä. 3DES:iä käyttämällä voidaan viesti salata kolme kertaa käyttäen kahta tai kolmea avainta, tämä parantaa turvallisuutta, sillä pelkän DES:n koko avainavaruus voidaan nykyaikaisin menetelmin käydä läpi alle vuorokaudessa. [8, s. 381.]

4.4 Salausjärjestelmät ja -protokollat

Salattujen yhteyksien muodostamiseksi tarvitaan salausjärjestelmiä jotka varmistavat sen, että tieto ei ole muuttunut matkalla, ja salatun yhteyden osapuolet ovat viestien lähettäjiä. Lisäksi salausjärjestelmät huolehtivat salakirjoituksesta. Salausjärjestelmien käyttöön voidaan vaatia erillistä ohjelmaa tai ne voivat toimia läpinäkyvästi omana kerroksenaan. Yhteyden molempien osapuolien tulee hallita käytetty salausprotokolla. [8, s. 388.]

4.4.1 SSL ja TLS

Secure Sockets Layer eli SSL-salausprotokolla on kehitetty 90-luvun puolivälissä Netscape Communications Corporationin toimesta. SSL:ää käytetään osapuolten todentamiseen sekä luottamuksellisuuden ja eheyden varmentamiseen. SSL on jakautunut Handshake ja Record Layer protokolliin. Handshake eli kättelyvaiheen protokolla perustuu siihen, että työasema ilmoittaa palvelimelle osaamansa salakirjoitusmenetelmät, joista palvelin valitsee käytetyn menetelmän ja ilmoittaa sen työasemalle. Osapuolet voidaan todentaa esimerkiksi käyttämällä erilaisia sertifikaatteja. Kättelyn ensimmäisessä vaiheessa sovitaan myös niin sanottu istuntoavain. Kättelyn päätyttyä kaikki viestit lähetetään käyttäen sovittua salausmenetelmää. TCP-protokollan päällä toimivan Record Layerin tehtäviin kuuluu viestien pakkaaminen ja osiointi sekä huolehtiminen eheydestä ja salakirjoittamisesta. Salaisen avaimen menetelmiä käytetään viestien salaamiseen ja eheyden varmistamiseen tiivistefunktioita. [8, s. 390–391.]

Tunnetuin SSL:n käyttöympäristö on WWW-sivustojen salaaminen HTTPS-yhteydellä eli http-protokolla on salattu käyttäen SSL:ää. Transport Layer Security eli TLS on jatkumoa SSL:lle, kun Netscape-yhtiö luopui protokollan kehityksestä.

4.4.2 SSH

Tiedonsiirron turvaamiseen kehitetty Secure Shellin yleisin käyttötapa on etäyhteys asiakasohjelmalla palvelimeen, jotta voitaisiin etäkäyttää toista konetta. SSH:ta voidaan käyttää myös muiden yhteyksien, kuten FTP:n tai HTTP:n tunnelointiin. SSH:lla on mahdollista käyttää useita algoritmeja salaukseen, sillä jos yhden yhteyden salaus saadaan purettua, käytettyä menetelmää ei voida suoraan käyttää muiden yhteyksien murtamiseen. [8, s. 388.]

SSH:n siirtokerros toimii TCP-protokollan päällä ja sen tehtävänä on huolehtia palvelimen ja työaseman tunnistuksesta sekä salakirjoituksesta ja viestien eheydestä. Kun yhteys muodostetaan käyttämällä SSH protokollaa, kaikki viestit salataan osapuolten välillä, vaikka tunnistusta ei ole vielä tapahtunut. Yhteyden välilleen muodostavat osapuolet sopivat käytetystä salakirjoitustavasta, pakkaustavasta, käytetystä tiivistefunktiosta, sekä menetelmästä palvelimen ja istuntoavaimen tunnistamiseksi. Kumpikin yhteyden osapuoli voi missä tahansa tilanteessa

vaatia käytettyjen menetelmien vaihtamista, kun uusista menetelmistä on sovittu, liikenne jatkuu normaalisti. [8, s. 389.]

Siirtoprotokollan päällä toimii niin sanottu käyttäjäntunnistuskerros. Käyttäjäntunnistuskerroksen tehtävänä on tunnistaa yhteyden osapuolet. Tunnistus voi tapahtua muun muassa käyttäjänimen ja julkisen avaimen perusteella, käyttäjänimen ja salasanan perusteella tai käyttäjänimen ja työaseman perusteella. Käyttäjäntunnistus- ja siirtoprotokollien päällä toimii yhteysprotokolla. Yhteysprotokollalla voidaan avata yhteyden sisäisiä kanavia, näitä kanavia voidaan käyttää kuten erillisiä yhteyksiä yhteyden tai pääteyhteyden välittämiseksi. [8, s. 390.]

4.5 Salatut etäyhteydet

Etätyöpöytäyhteys on tässä työssä tarkoitus toteuttaa kahden tietokoneen välillä lähiverkossa ja tällöin ei tyypillisesti käytetä VPN- tai HTTPS-yhteyksiä, jotka tässä esitelläänkin lähinnä periaatteellisella tasolla.

Etäkäyttötilanteessa, jossa muodostetaan yhteys esimerkiksi lähiverkkojen välille julkisen verkon yli, joudutaan usein käyttämään salattua yhteyttä. Turvallisen yhteyden mahdollistamiseksi, tietoliikenne salataan esimerkiksi HTTPS-protokollalla tai vaihtoehtoisesti käyttämällä VPN:ää eli suojattua verkkoyhteyttä [3, s. 39].

VPN-yhteydessä Internet toimii esimerkiksi kahden erillisen lähiverkon yhdyskäytävänä, jolloin lähiverkkojen välinen liikenne lähetään IP-datapakettien sisällä salattuna [8, s. 284–285]. VPN voidaan määrittää esimerkiksi väliaikaiseksi fyysiseksi reitiksi, joka on muodostettu julkisen verkon yli. VPN-yhteys muodostetaan yleensä verkon reitittimien välille, jolloin lähettävä reititin kapseloi datan salattuna IP-pakettiin ja lähettää tämän verkon yli vastaanottavalle reitittimelle, joka useimmiten purkaa kapseloinnin ja lähettää datan salaamattomana vastaanottavalle laitteelle lähiverkossa [8, s. 285]. VPN-yhteyksien muodostuksessa käytetään useita protokollia, jotka toimivat OSI-mallin eri kerroksilla.

5 ETÄTYÖPÖYTÄJÄRJESTELMÄN TOTEUTUS

Tässä luvussa tarkastellaan etätyöpöytäjärjestelmän toteutusta sekä sitä, kuinka lähiverkkoratkaisu toteutettiin ja millaisia ohjelmia on olemassa etäyhteyden muodostamiseksi. Tavoitteena oli suunnitella ja toteuttaa etäkäyttöympäristö, jossa etätyöpöytäyhteyttä käyttäen hallitaan tietokonetta, sekä sen laitteita, ohjelmistoja ja siirretään tiedostoja koneiden välillä.

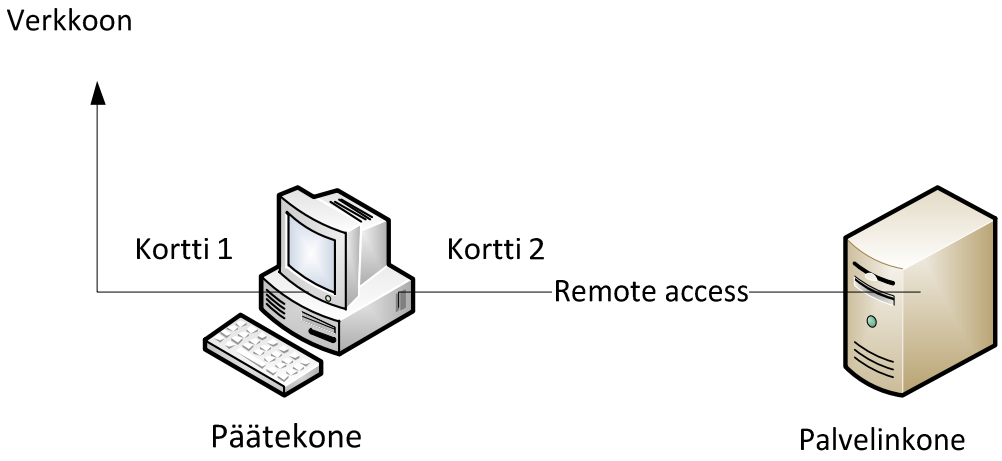
5.1 Verkkoympäristön kuvaus

Verkkoympäristö toteutettiin kuvan 8 mukaisesti. Järjestelmässä oli kaksi tietokonetta, joista toinen oli niin sanottu päätekone (client), jolla hallittiin toista tietokonetta, josta tässä käytetään nimitystä palvelinkone (server). Palvelinkoneen ohjelmistoja ja laitteita hallittiin etätyöpöytäyhteyden kautta. Päätekoneeseen kytkettiin olemassa olevan verkkokortin (kortti 1) lisäksi toinen verkkokortti (kortti 2), jonka tehtävänä oli huolehtia etäyhteydestä palvelinkoneelle.

Päätekoneen toisena verkkokorttina käytettiin USB –verkkosovitinta malliltaan Wintech-LAU-15-USB-2.0-LanCard, joka kytkettiin palvelinkoneeseen ristiin kytketyllä CAT-5-verkkokaapelilla. Vaihtoehtoisesti verkkosovittimena olisi voitu käyttää muihinkin tietokoneen väyliin, kuten PCI- ja PCI-E -väyliin tarkoitettuja verkkokortteja. Päätekoneen käyttöjärjestelmänä oli 64-bittinen Windows-7-Enterprise- ja palvelinkoneen Windows-XP-Professional -käyttöjärjestelmä, jotka olivat ennalta asennettuina molempiin etäkäyttöverkon koneisiin. Molempia käyttöjärjestelmiä käytettiin järjestelmänvalvojan käyttöoikeuksilla.

Palvelinkoneen Windows-XP käyttöjärjestelmään kirjautuminen automatisoitiin, jotta tarvittaessa kyseisen tietokoneen syöttö- ja tulostuslaitteet, kuten näyttö ja näppäimistö voitaisiin poistaa käytöstä. Kirjautumisen automatisointi toteutettiin muokkaamalla käyttöjärjestelmän rekisteritietokantaa rekisterieditorilla, siten että käytetyn käyttäjätilin salasana (DefaultPassword) ja käyttäjätunnus (DefaultUserName) tallennettiin rekisteriin, jonka avain oli HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrenVersion\Winlogon.

Automaattinen kirjautuminen (AutoAdminLogon) vahvistettiin, antamalla sille arvo 1 (tosi). On kuitenkin huomioitava automaattisesta kirjautumisesta aiheutuva tietoturvariski, sillä näillä asetuksilla kaikki käyttäjät voivat käyttää palvelinkonetta järjestelmänvalvojan käyttöoikeuksilla.

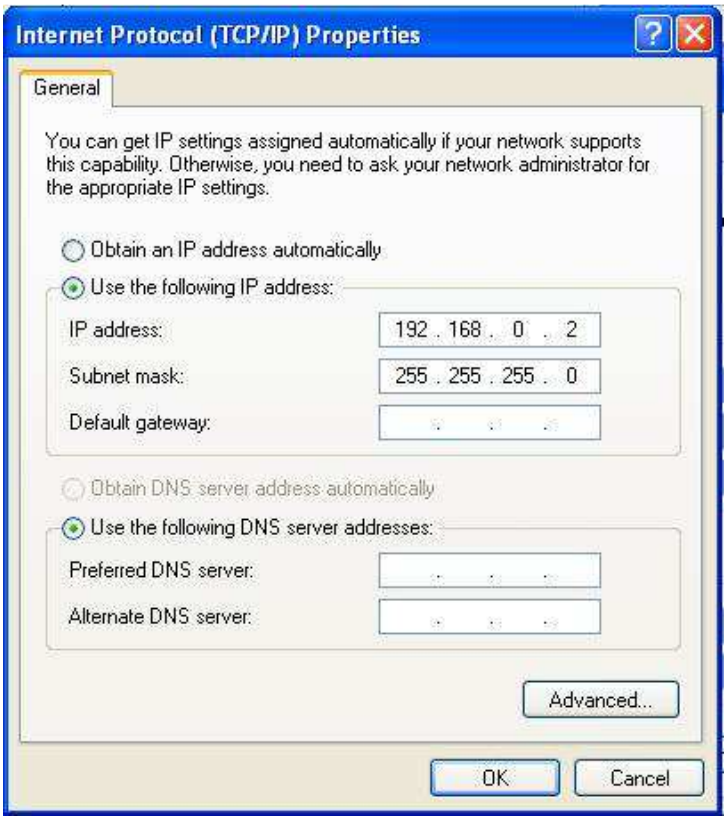


Kuva 8. Verkkokorttiratkaisu etäkäyttöympäristön toteuttamiseksi.

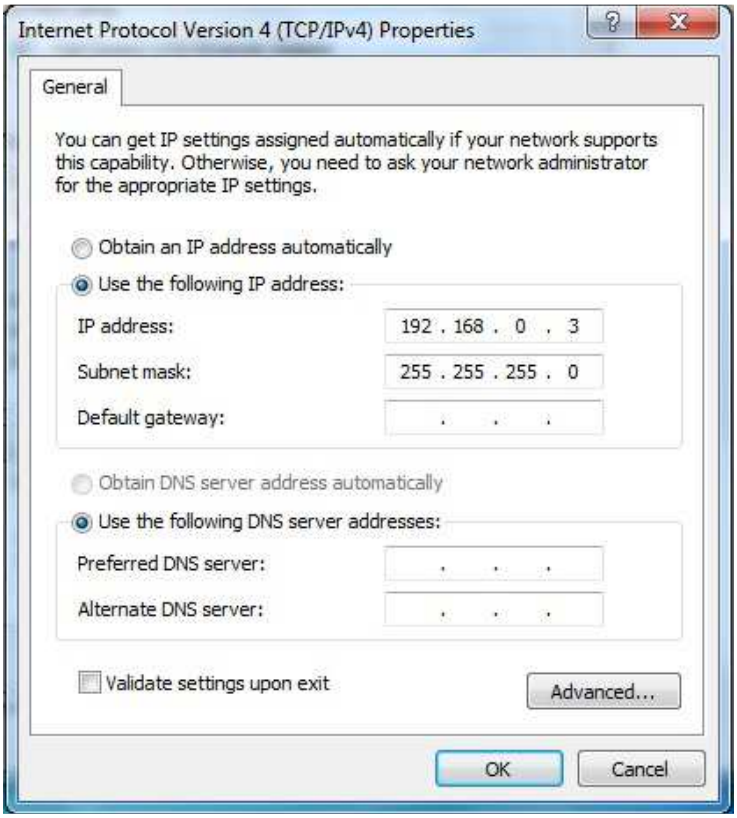
5.1.1 Verkkoasetukset

Molemmille etäkäyttöverkon verkkokorteille palvelin- (kuva 9) ja päätekoneissa (kuva 10) määritettiin kiinteät IP-osoitteet(IPv4) verkkokorttiasetuksista. Osoitteiksi valittiin RFC1918:n, määrittämän yksityisosoitealueen 192.168.0.0 – 192.168.255.255 IP-osoitteet [18, s. 4]. Palvelinkoneen osoitteeksi asetettiin 192.168.0.2 ja päätekoneen osoitteeksi 192.168.0.3. Verkon peitteelle joka ilmaisee, mikä osa IP-osoitteesta on verkon osoitetta, annettiin arvo 255.255.255.0. Yhdyskäytävä eli Default Gateway jätettiin tyhjäksi, sillä etäyhteysverkon verkkosovittimien välistä liikennettä ei reititetä muualle.

Päätekoneen etäyhteyskortin verkkoasetuksista poistettiin IPv6 käytöstä, koska sitä ei käytetty tässä tapauksessa lainkaan. Päätekoneen verkkokortti (kortti 1, kuva 8), joka huolehtii verkkoyhteydestä organisaation verkkoon ja tästä eteenpäin, käyttää dynaamista IP-osoitetta, joka jaetaan laitteelle erikseen DHCP-palvelimen toimesta. Tämän verkkokortin asetuksiin ei puututtu.



Kuva 9. Palvelinkoneen IP–asetukset.



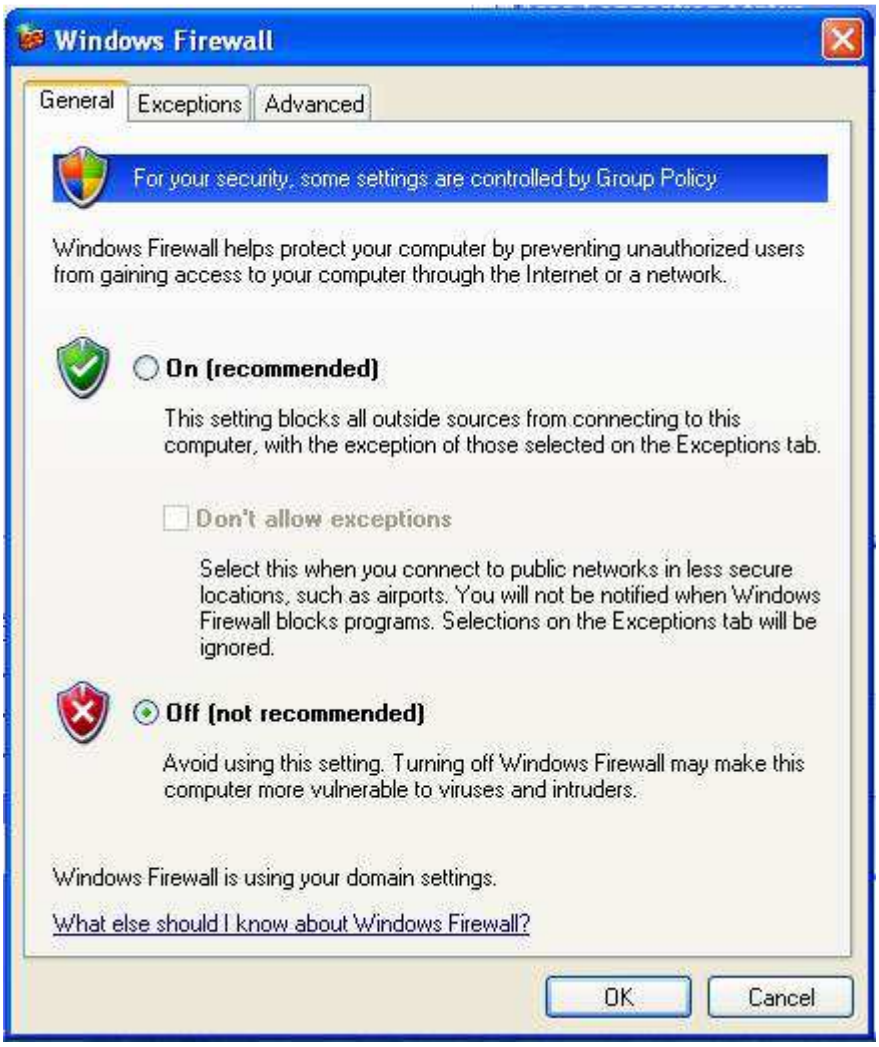
Kuva 10. Päätekoneen IP-asetukset.

Verkkoyhteyden toimintaa testattiin alkuvaiheessa ”pingaamalla” kohdekonetta, sekä päätettä että palvelinkoneelta. Ping on ICMP-viestejä lähettävä ohjelma, joka sisältyy TCP/IP:hen. Yleensä Pingiä käytetään kaiutuspyyntöjen lähettämiseen aktiivilaitteille tai koneille verkon tilan selvittämiseksi [8, s. 267]. Yhteys todettiin muodostetuksi, kun ”pingaus” onnistui molempiin suuntiin eli päätekoneelta palvelinkoneelle ja päinvastoin.

5.1.2 Palomuuriasetukset

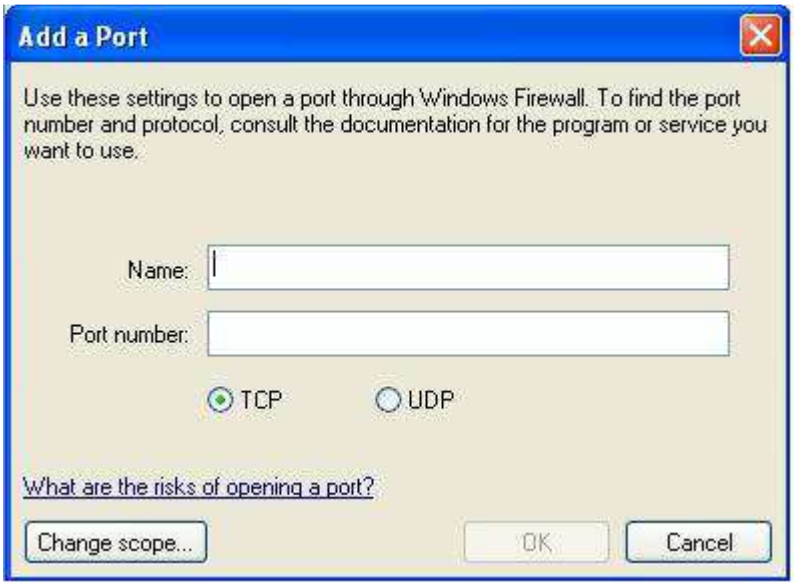
Molemmat etäkäyttöverkon tietokoneet (kuva 8) käyttävät Windowsin omaa palomuuriohjelmistoa (Windows Firewall). Windowsin-palomuuri on ohjelmallinen palomuuri- ja pakettisuodatinsovellus, joka on sisäänrakennettuna Windows -käyttöjärjestelmissä alkaen Windows-XP:stä (Service Pack 2) [19]. Palomuuriasetukset toteutettiin käytännössä siten, että liikenne etäyhteysprotokollien määrittämiin portteihin olisi sallittua, esimerkiksi RDP –protokolla käyttää oletuksena TCP-porttia 3389 [5, s. 32] ja RFB –protokolla porttia 5900 tai 5500 (palvelimelta asiakkaalle) [20, s. 3]. Windowsin-palomuuriasetuksista voidaan sallia tai estää tiettyjen ohjelmien toiminta, yhteydet tiettyihin portteihin tai mahdollisesti sulkea koko palomuuri, jolloin luonnollisesti kaikki liikenne on sallittua verkon ja tietokoneen välillä.

Johtuen verkon rakenteesta eli palvelinkone on käytännössä yhteydessä ainoastaan päätekoneen USB-verkkosovittimeen parikaapelin kautta, palvelinkoneen palomuuriasetukset voidaan pitää kevyehköinä tai mahdollisesti palomuuri voidaan sulkea kokonaan (kuva 11). Palomuurin sulkeminen kokonaan asettaan tietokoneen kuitenkin erittäin haavoittuvaan tilaan ja mahdollistaa erilaisten haittaohjelmien ja virusten leviämisen järjestelmään, vaikkakaan verkkoyhteyttä julkiseen verkkoon ei ole. Leviämiskanavana haittaohjelmille tässä tapauksessa voidaan pitää muun muassa tallennusmedioita, kuten USB-muistitikkuja.



Kuva 11. Palvelinkoneen palomuuri pois käytöstä (Win-XP).

Jos palvelinkoneen palomuuri on käytössä, ohjelmia tai toimintoja voidaan sallia palomuuriasetusten kohdasta Exceptions (poikkeukset) tai määrittämällä portti johon yhteydet sallitaan (kuva 12). Riippumatta palomuuriasetuksista remote desktop connection eli etätyöpöytäyhteyden tulee olla sallittu palvelinkoneella. Käytettäessä muita etätyöpöytäohjelmistoja, kuin Windowsin etätyöpöytää (luku 6.1), ohjelmat tekevät yleensä itse muutoksia palomuuriasetuksiin sallimalla liikenteen käyttämiinsä TCP-portteihin.

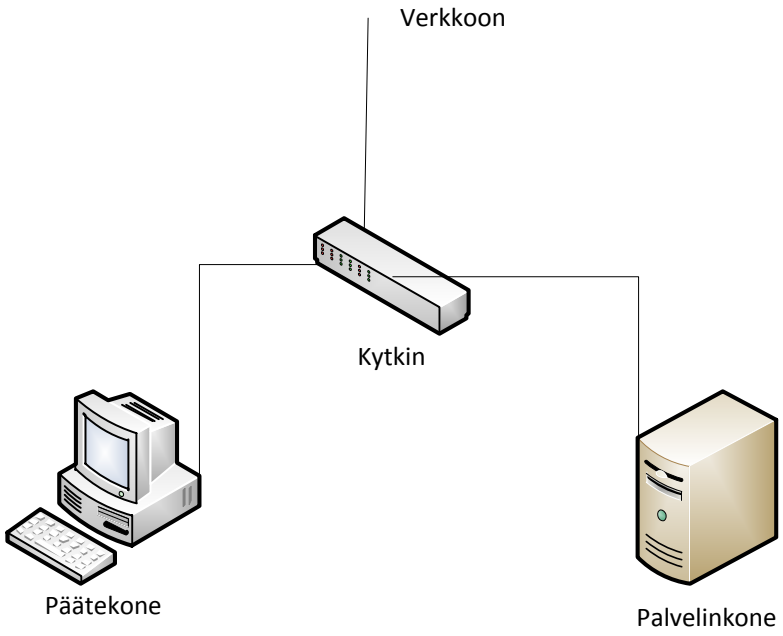


Kuva 12. Yhteyden salliminen tiettyyn porttiin palvelinkoneessa (Win-XP).

Päätekone on yhteydessä myös organisaation verkkoon ja siitä eteenpäin, joten palomuuriasetusten tulee olla tiukemmat, kuin palvelinkoneessa. Jos päätekoneeseen ei tarvitse ottaa etäyhteyttä, muutoksia palomuuriasetuksiin ei tarvita. Mikäli jossakin tilanteessa etätyöpöytäyhteys päätekoneelle tulisi muodostaa, sallitaan Remote Desktop Connection palomuuriasetuksista tai järjestelmäasetusten (System Properties) Remote-asetuksista.

5.2 Vaihtoehtoiset verkkoratkaisut

Verkkoyhteys koneiden välille voidaan muodostaa useilla eri tavoin. Luvussa 5.1 esitellyn tavan lisäksi testattiin myös kuvan 13 mukaista järjestelmää, jossa verkon aktiivilaite, joka tässä tapauksessa oli Cisco-SD2005-5-port-Gigabit -verkkokytkin, yhdisti tietokoneet verkkoon.



Kuva 13. Kytkimellä toteutettu verkkoratkaisu.

Palomuuriasetukset olivat päätekoneen osalta samat kuin luvussa 5.1 esitetyt, mutta palvelinkoneen palomuuriasetuksia tiukennettiin siten, että sallittiin ainoastaan etätyöpöytäyhteyden muodostus, koska tässä tapauksessa myös palvelinkone olisi kytkimen kautta yhteydessä organisaation verkkoon.

Ongelmaksi tässä tapauksessa muodostui IP-osoitteiden hallinta ja uuden verkkolaitteen tuonti verkkoon, sillä palvelinkoneessa käytettiin edelleen kiinteää IP-osoitetta, mikä aiheutti ristiriitatilanteita verkossa. Palvelinkoneen kuormitus haluttiin pitää kohtuullisen matalana ja raskaiden turvaohjelmistojen käyttöä haluttiin välttää, sillä niiden havaittiin hidastavan järjestelmän toimintaa kohtuuttoman paljon. Lisäksi etäyhteyden toiminnan kannalta palvelinkoneen ei tarvitse keskustella muiden laitteiden, kuin päätekoneen välillä. Mikäli tämän tyyppinen verkko haluttaisiin toteuttaa, kytkimen tai vastaavan verkon aktiivilaitteen tulisi olla konfiguroitavissa siten, että palvelinkone näkyisi ainoastaan päätekoneelle. Kuvan 13 mukainen verkkoratkaisu olisi toimiva esimerkiksi kotiverkossa, mutta tämäntyyppisessä tilanteessa luvussa 5.1 esitetty verkkoympäristön toteutustapa on mielekkäämpi.

Oletettavaa on myös se, että tämän tyyppinen verkkoratkaisu tulisi todennäköisesti kalliimmaksi, kuin verkkosovittimilla toteutettava ratkaisumalli, ainakin jos toteutus tehtäisiin laajemmassa mittakaavassa.

6 ETÄTYÖPÖYTÄOHJELMISTOT

Erilaisia etäkäyttö- ja etätyöpöytäohjelmistoja on olemassa sekä ilmaisia että maksullisia, jotka pohjautuva protokolliin, kuten RFB ja RDP. Tässä luvussa tarkastellaan ja vertaillaan kolmea eri etäkäyttöohjelmistoja, joilla voidaan toteuttaa etätyöpöytäyhteys pääte- ja palvelinkoneen välille. Ohjelmistotesti ja vertailu suoritettiin Windows-etätyöpöydällä, TightVNC:llä ja TeamViewerillä. Vaatimuksena ohjelmistoille oli toiminta käyttöjärjestelmillä MS-Windows-7 ja –XP, tiedostojen vaihto koneiden välillä sekä ohjelmistojen turvallisuus. Ohjelmistot testattiin luvussa 5.1 määritellyillä verkko- ja palomuuriasetuksilla.

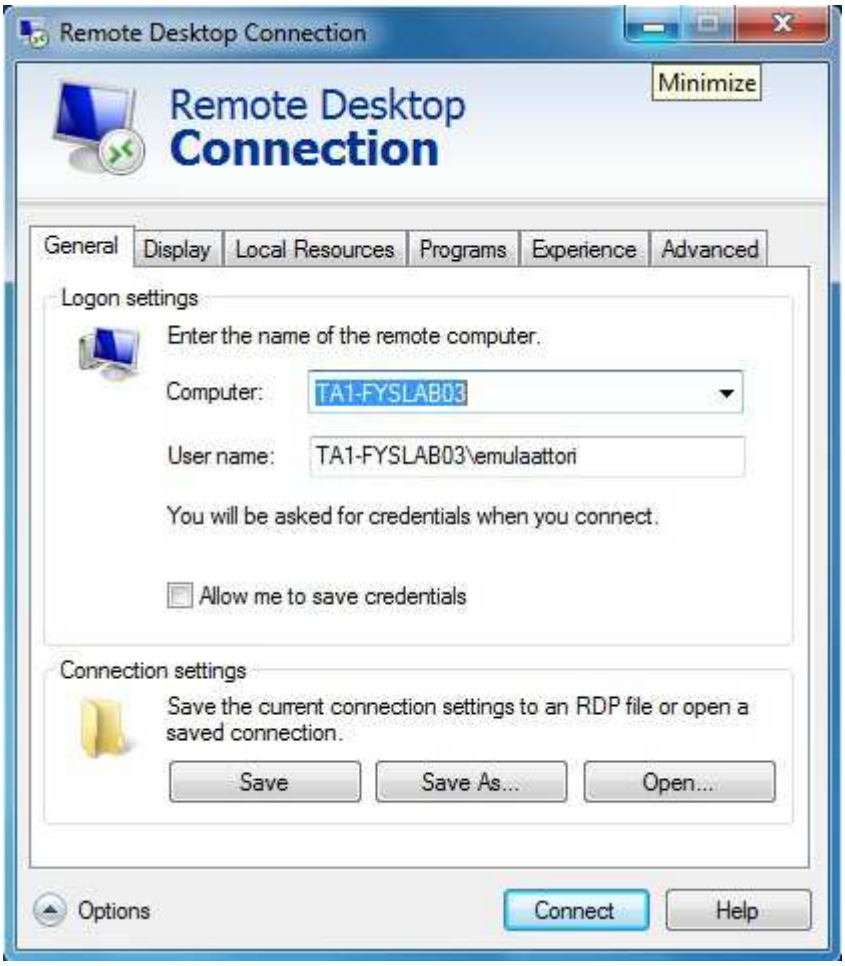
Ohjelmistoja tarkasteltiin lähinnä yhteyden muodostuksen ja ohjelmakohtaisten asetusten määrittämiseen kannalta siten, että ne toteuttaisivat yhteydelle asetetut vaatimukset. Esimerkiksi ohjelmistojen asennukseen ei kiinnitetty juurikaan huomiota, sillä siihen ei liittynyt käytettyjen ohjelmistojen osalta mitään huomioitavaa.

6.1 Microsoft Windows Remote Desktop Services eli Windows-etätyöpöytä

Remote Desktop Services on MS Windowsin komponentti palvelin ja asiakasohjelmistoissa, kuten Windows Server 2008 ja Windows 7. Remote Desktop Services mahdollistaa etäkoneen sovellusten ja tietojen käytön verkon yli. Yhteyden muodostamiseen ja ylläpitämiseen käytetään Remote Desktop protokollaa. Etätyöpöytää ei tarvitse erikseen asentaa, koska se on asennettu varsinaisen käyttöjärjestelmän asennuksen yhteydessä. Remote Desktop Services tunnettiin aiemmin nimellä Terminal Services, joka esiteltiin ensimmäisen kerran osana Windows NT 4.0:aa. Yhteydenmuodostuksesta etäkäytettävän palvelinkoneen päässä huolehtii ohjelman osa Terminal Server, joka tunnistaa asiakkaan (client) ja mahdollistaa ohjelmien etäkäytön palvelinkoneelta.[21.]

Windows-7:n etätyöpöytäasiakkaan Remote Desktop Connection kirjautumisikkunasta (kuva 14) määritetään kone johon etäyhteys muodostetaan käyttämällä koneen nimeä ja käyttäjänimeä tai IP-osoitetta. Tiedot muodostettavan yhteyden asetuksista voidaan tallentaa, jotta niitä ei tarvitse määrittää uudestaan jokaiselle kerralle. Näyttöasetuksia hallitaan Display-välilehdeltä, josta voidaan muun muassa valita kuinka suurena etätyöpöytäikkuna näytetään ja minkälaisia väriasetuksia käytetään. Paikallisia resursseja, kuten näppäimistöä ja muita laittei-

ta, sekä levyasemien jakoa etätyöpöytäistunnossa hallitaan kohdasta Local Resources. Programs-välilehdeltä valitaan ohjelma, joka mahdollisesti halutaan käynnistää yhteyden muodostuksen yhteydessä. Experience-välilehdeltä voidaan valita käytetty yhteyden nopeus suorituskyvyn maksimoinniksi, esimerkiksi tässä tapauksessa kun oli kyse lähiverkkoyhteydestä (kuva 8), valittiin kyseinen yhteystapa sekä sallittiin muun muassa taustakuvan näyttäminen, ja ikkunoiden sekä valikon animaatiot.

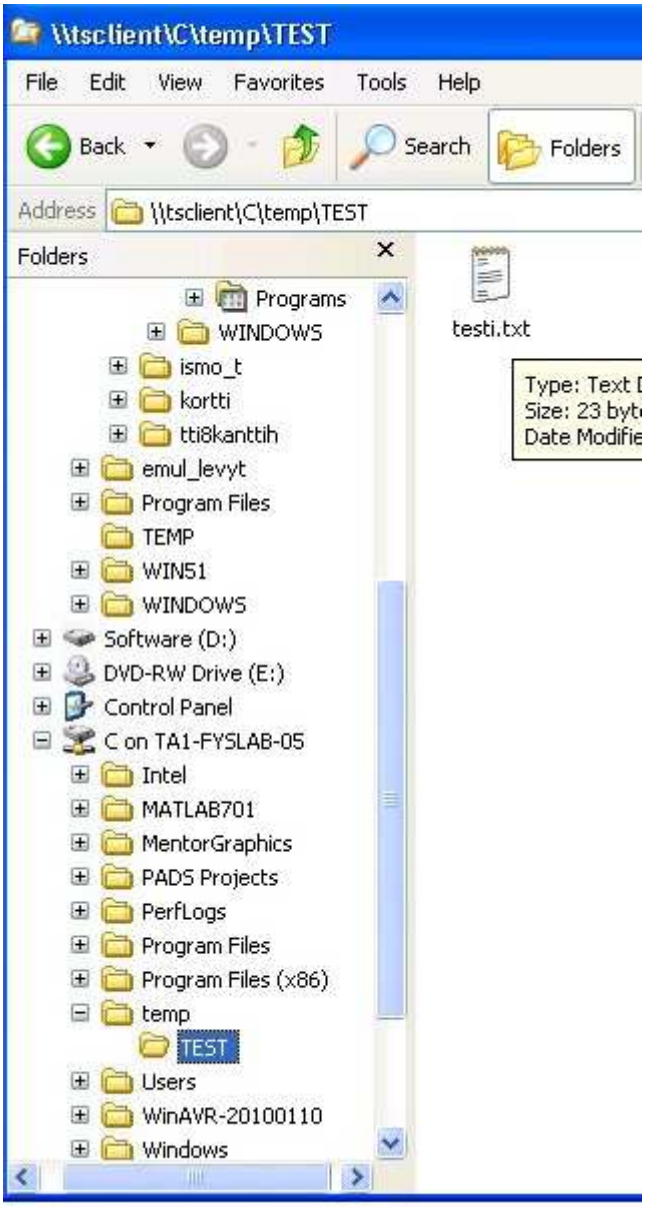


Kuva 14. Windows 7 etätyöpöytäasiakas.

Yhteyttä muodostettaessa etäkäytettävään palvelinkoneeseen havaittiin, että päätekoneen verkkoasetuksista tuli estää muiden kuin etäyhteysverkkokortin toiminta. Kun yhteys pyrittiin muodostamaan tilanteessa, jossa päätekoneen molemmat verkkokortit olivat toiminnassa, etätyöpöytä lähetti etäyhteyskutsun tietokoneen varsinaisen verkkokortin kautta (kortti 1, kuva 8), jolloin ei havaittu palvelinkonetta etäyhteysverkossa. Etäyhteyden muodostuksen jälkeen varsinainen verkkokortin toiminta voitiin sallia, jolloin päätekoneella voitiin olla yhteydessä Internetiin ja organisaation verkkoon.

Yhteyttä muodostettaessa palvelinkoneelle tuli siihen kirjautua palvelinkoneen Windowsin käyttäjätunnuksella ja salasanalla.

Etäyhteyden eräänä vaatimuksena oli tiedostojen siirto pääte- ja palvelinkoneen välillä. Tiedostojen siirtoa testattiin luomalla tiedosto, joka tässä tapauksessa oli txt-tiedosto nimeltään testi.txt, joka tallennettiin päätekoneen C: asemalle. Etäyhteyden kautta tiedosto avattiin palvelinkoneella (kuva 15).



Kuva 15. Päätekoneen tiedosto avattuna palvelinkoneella etäyhteyden kautta.

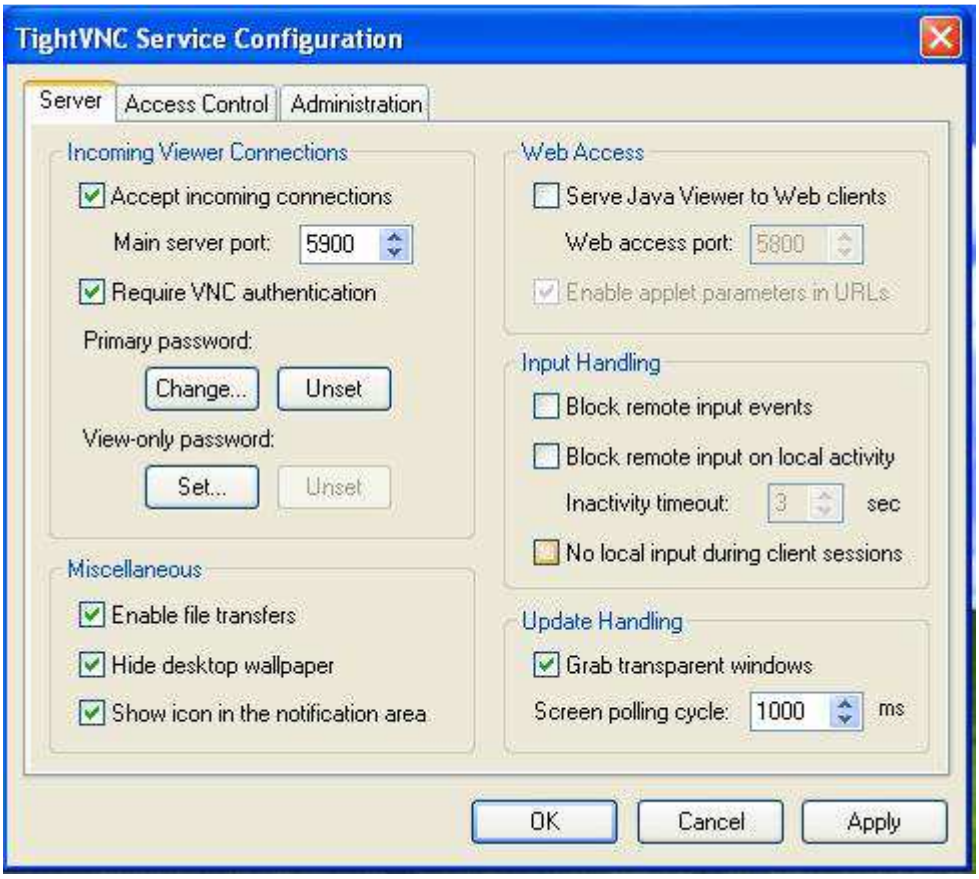
Tiedostonvaihdon lisäksi testattiin palvelinkoneiden eräiden ohjelmien suoritus etätyöpöytäyhteyden kautta. Ohjelmat toimivat pääosin hyvin, mutta johtuen tiedonsiirrosta etäyhteydessä, palvelinkoneen ohjelmien toiminnassa havaittiin pientä viivettä, joka voi johtua myös palvelinkoneen vajavaisesta suorituskyvystä tai USB-verkkosovittimen hitaudesta.

6.2 TightVNC

TightVNC on ilmainen RFB-protokollaan perustuva etähallinta- ja etätyöpöytäohjelmisto, joka toimii sekä Windows, että UNIX-pohjaisilla käyttöjärjestelmillä [22]. Ohjelmisto koostuu kahdesta osasta Service ja Viewer, jotka molemmat voidaan määrittä asennettaviksi yhdessä tai erikseen asennuksen yhteydessä. ”Service” eli ohjelman osa, joka mahdollistaa etätyöpöytäyhteyden muodostuksen kyseiselle laitteelle, asennetaan siihen koneeseen, jota etäkäytetään. Viewer:in avulla otetaan yhteys koneeseen jota halutaan etäkäyttää ja johon on asennettuna TightVNC-Service.

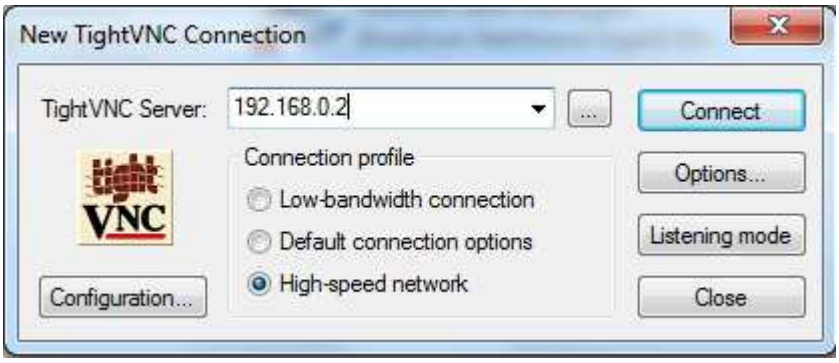
TightVNC ladattiin ohjelman verkkosivuilta [22]. Ohjelman Service osa asennettiin palvelinkoneelle ja Viewer päätekoneelle.

TightVNC Viewerin konfigurointitilasta (kuva 16) sallittiin tulevat yhteydet porttiin 5900, sekä vaadittiin autentikointia etäkäyttäjältä eli päätekoneen käyttäjältä. Lisäksi sallittiin tiedostojenvaihto ja piilotettiin palvelinkoneen taustakuva.



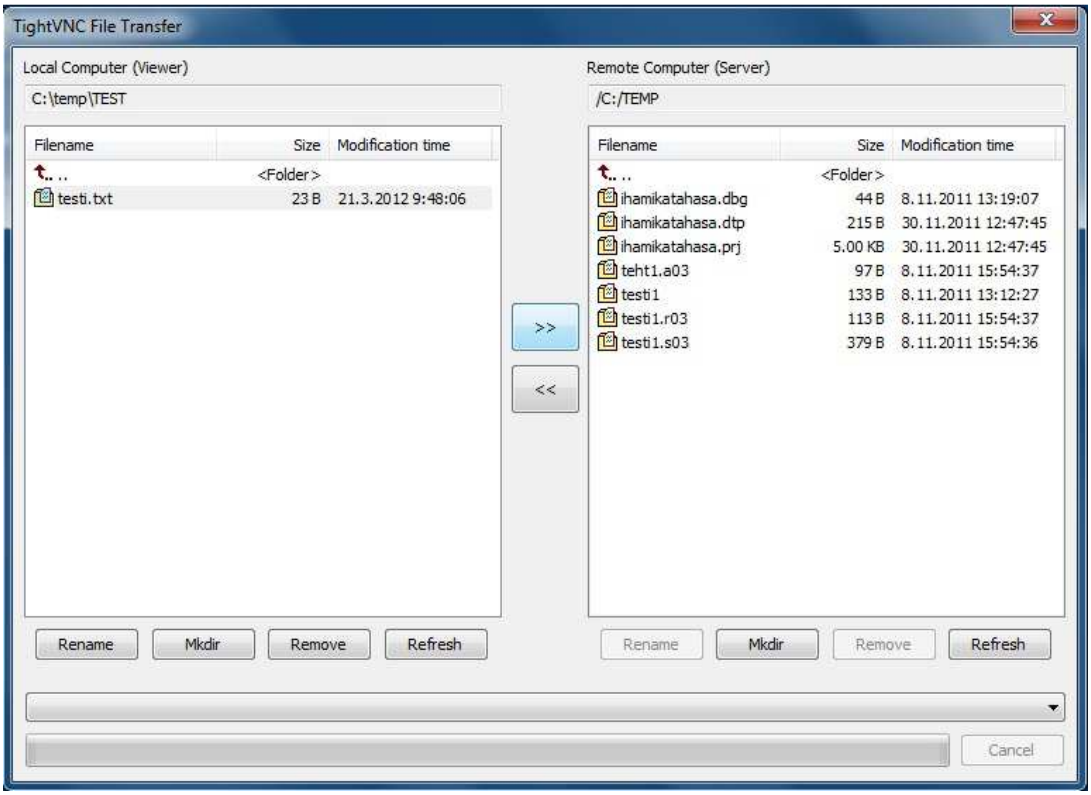
Kuva 16. TightVNC Service konfiguraatio

Päätekoneelle asennetun Viewerin pääikkunasta (kuva 17) syötettiin palvelinkoneen IP-osoite 192.168.0.2, johon yhteys haluttiin muodostaa. Yhteysmuodoksi asetettiin nopea verkkoyhteys High-speed network.



Kuva 17. TightVNC Connection, yhteydenmuodostus.

Yhdistettäessä palvelinkoneelle vaadittiin salasanaa, joka oli asetettu palvelinkoneen Service configuration asetuksissa. Salasanaksi oli tässä tapauksessa asetettu *testi*. Tiedostojen vaihtoa testattiin, kuten Windowsin etätyöpöydän yhteydessä eli päätekoneella luotu tiedosto ”testi.txt” siirrettiin palvelinkoneelle (kuva 18).



Kuva 18. TightVNC tiedostojen siirto.

Palvelinkoneen ohjelmistojen käyttö etätyöpöytäyhteyden kautta oli suhteellisen nopeaa, kun yhteyden ominaisuuksia rajoitettiin. TightVNC käyttö oli kaiken kaikkiaan erittäin sujuvaa ja helppoa. Lisäksi huomioitavaa oli se, että toisin kuin Windows etätyöpöydän yhteydessä, päätekoneen verkkoasetuksiin ei tarvinnut puuttua missään vaiheessa.

6.3 TeamViewer

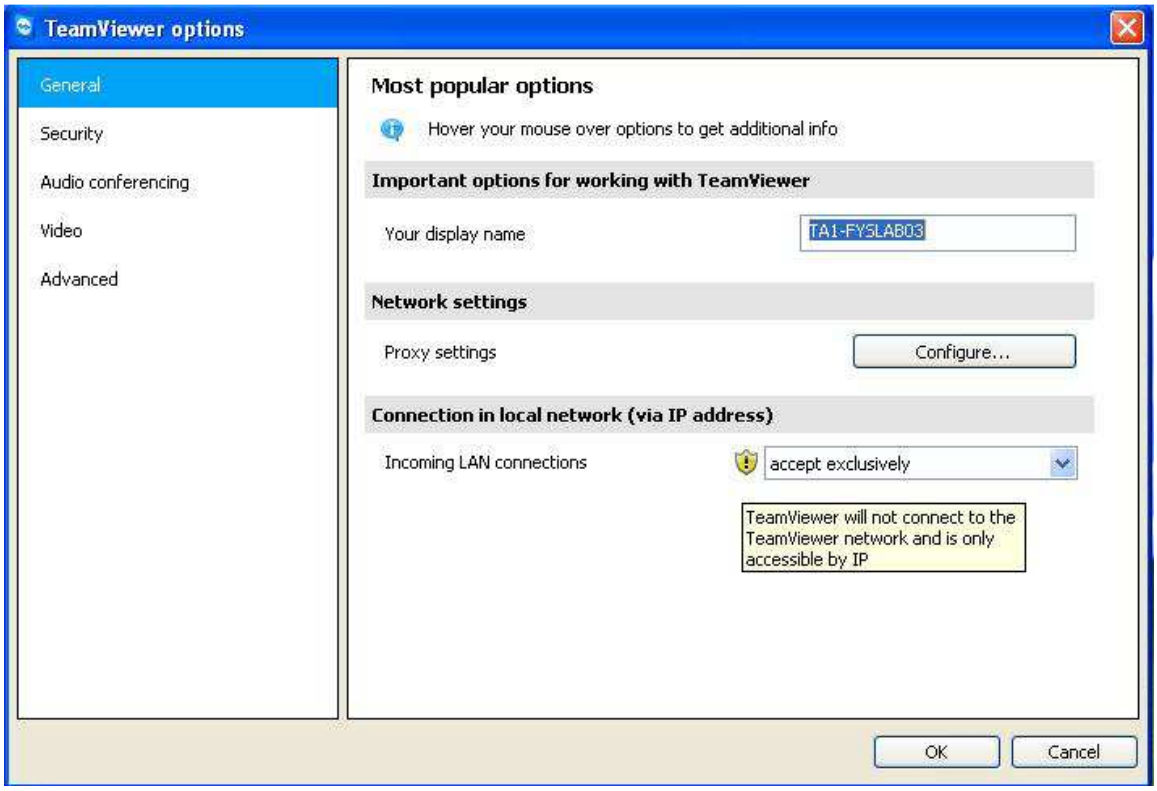
TeamViewer on ei-kaupallisessa käytössä ilmainen etähallintaohjelmisto, joka Windowsin lisäksi toimii myös Linux ja Mac -ympäristöissä. Etähallinnan lisäksi TeamViewer:iä on mahdollista käyttää etätuen työkaluna, sekä työryhmätyöskentelyyn verkon yli.

TeamViewerin verkkosivuilta [23] asennettiin päätekoneelle TeamViewerin versio 7.0 ja palvelinkoneelle ohjelman versio TeamViewer-Host, joka on tarkoitettu valvomattomille palvelimille ja mahdollistaa jatkuvan etäkäytön.

Päätekoneelle asennetun TeamViewerin hallintaikkunasta (kuva 19) voidaan nähdä päätekoneen ID, joka tässä tapauksessa oli kyseisen koneen etäkäyttöverkkokortin IP-osoite. TeamViewerin asetuksista (Options) määritettiin ainoastaan lähiverkko- eli LAN-yhteydet sallituiksi. Lisäksi estettiin yhteydenmuodostus päätekoneelle. Palvelinkoneen IP-osoite syötettiin kohtaan Partner ID ja yhteystavaksi valittiin etähallinta eli Remote Control.

Kuva 19. TeamViewer pääikkuna päätekoneella.

Palvelinkoneelle asennettiin TeamViewerin Host -version, jonka asetuksista estettiin myös muut kuin lähiverkkoyhteydet (kuva 20). Lisäksi asennuksen yhteydessä määritettiin salasana, jota tulee käyttää kun yhteys muodostetaan päätekoneelle.



Kuva 20. TeamViewer Host, LAN-yhteys sallittu.

Käyttäjän tunnistuksessa yhteyden muodostuksessa voidaan käyttää TeamViewerin omaa salasanaa tai Windowsin käyttäjänimeä ja salasanaa. Tässä tapauksessa käytettiin TeamViewerin salasanaa. Palvelinkoneen käyttöoikeuksia voidaan rajoittaa, mutta testattaessa ohjelmistoa sitä käytettiin rajoittamattomasti Full Access -oikeuksilla, täytyy kuitenkin huomata, että palvelinkoneen TeamViewer Hostin asetuksista tulee Full Access olla sallittuna.

Tiedostojenvaihto testattiin, kuten Windowsin etätyöpöydän ja TightVNC:n ja tapauksessa eli päätekoneen txt-tiedosto siirrettiin palvelinkoneelle. Tiedostojen vaihto ja palvelinkoneen ohjelmien käyttö onnistui ongelmitta. Kuten TightVNC:llä, myöskään TeamViewerin yhteyden muodostuksessa päätekoneen verkkoasetuksiin ei tarvinnut puuttua.

6.4 Vertailu

Taulukossa 3 on vertailtu aiemmin testattuja etäkäyttöohjelmistoja. Vertailukohtina valituille ohjelmistoille valittiin käytetty (etäkäyttö-) protokolla, salausmenetelmät, tuetut käyttöjärjestelmät tiedostojen siirto koneiden välillä, sekä hinta.

Taulukko 3. Etätyöpöytäohjelmistojen vertailua.

OHJELMISTOVERTAILU	**Protokolla**	**Salausmenetelmä(t)**	**Käyttöjärjestelmät**	**Tiedostojensiirto**	**Hinta**
Windows etätyöpöytä	RDP	RC4, TLS	Windows, palvelin- ja asiakasohj.	X	
TightVNC	RFB	DES	Windows, UNIX	x	
TeamViewer	-	RSA,AES-256	Windows, Linux, Mac	x	

Testatuista ohjelmistoista Windows etätyöpöytä käyttää RDP-protokollaa ja TightVNC RFB-protokollaa, jotka on esitelty aiemmin tässä dokumentissa. TeamViewer ei varsinaisesti käytä mitään erikseen määriteltyä etäkäyttöprotokollaa. Peruskäytössä eri protokollien pohjilta kehitettyjen ohjelmistojen toiminnassa ei havaittu eroa.

Salausmenetelmiä vertailtaessa TightVNC on kolmikosta ”kevyin”, sillä ainoastaan salasanat on salattu käyttäen DES-salausta, jonka efektiivinen avainpituus on 56-bittiä. Varsinainen liikenne lähetetään salaamattomana verkossa ja tästä johtuen TightVNC:n tekijätkin suosittelevat käyttämään turvattomissa verkoissa SSH-tunnelointia [24]. Windows etätyöpöytä käyttää maksimissaan 128-bittistä RC4-algoritmin mukaista salausta. Lisäksi Windows etätyöpöytä tukee TLS-1.0 -salausprotokollaa, sekä palvelin- että asiakaspäissä, jota ei kuitenkaan käytetä oletuksena vaan siitä on sovittava erikseen yhteyden osapuolten välillä. TeamViewerin turvallisuus perustuu RSA:n yksityisen ja julkisen avaimen menetelmään ja AES:n 256-bittiseen istuntosalaukseen. Windows-etätyöpöydän ja TeamViewerin turvallisuutta vertailtaessa, todettiin molempien olevan jo perusominaisuuksiensa perusteella suhteellisen turvallisia.

Kuten aiemmissa vaiheissa kävi ilmi, kaikki testatut ohjelmistot toimivat luvussa 5.1 määritellyssä verkkoympäristössä, jossa päätekone käyttää Windows 7- ja palvelinkone Windows XP -käyttöjärjestelmää. TightVNC toimii Windows käyttöjärjestelmien lisäksi myös UNIX ym-

päristöissä. TeamViewer toimii myös Mac-laitteilla ja verkon kautta myös erilaisilla mobiilikäyttöjärjestelmillä.

Tiedostojensiirto onnistui kaikilla testatuilla etäkäyttöohjelmistoilla ja tiedostonsiirron todettiin olevan yksinkertaista ja helppoa. Vertailtaessa ohjelmistojen hintaa todetaan, että Windows etätyöpöytä on olemassa oleva komponentti Windowsin ohjelmistoissa, joten sen hankinnasta ja käytöstä ei aiheudu erillisiä kustannuksia. TightVNC on ilmainen, sekä yksityisessä, että kaupallisessa käytössä. Kyseistä ohjelmistoa kehittävän tahon tulonhankintalogiikkana on erilaisten tukipalveluiden myynti ohjelmiston käyttäjille. TeamViewer on ilmainen eikaupallisessa käytössä. Kaupalliseen käyttöön TeamViewerillä on tarjota kolme eri tason lisenssivaihtoaehtoa, joista halvin on hinnaltaan noin 500 euroa ja kallein Corporate lisenssi noin 2000 euroa.

Windows etätyöpöydän edut ja haitat:

- Ilmainen.
- Ei vaadi erillisiä ohjelmistoasennuksia.
- Helppokäyttöinen.
- Testatussa käytössä riittävän suorituskykyinen.
- Ongelmia aiheutui yhteydenmuodostuksessa.

TightVNC edut ja haitat:

- Ilmainen
- Verrattain hidas, mutta yhteyden ominaisuuksia rajoittamalla, esimerkiksi taustakuvan piilottamisella saavutettavissa riittävä nopeus.
- Haittana, vanhahtava toteutustapa ja protokolla, sekä turvallisuus.

TeamViewer edut ja haitat:

- Maksullinen
- Etuna hyvä turvallisuuden toteutus, kohtuullinen nopeus sekä selkeä käyttöliittymä.
- Ohjelman käyttö ei vaadi muutoksia palomuuriasetuksiin.

7 TULOSTEN TARKASTELU

Tässä luvussa tarkastellaan työn tuloksia ja jatkokehitysideoita.

7.1 Tulokset

Tämän dokumentin luvussa 5.1 esitellyn tavan mukainen verkkoratkaisu on yksinkertaisin ja mahdollisesti myös helpoin keino toteuttaa etäkäyttöratkaisu haluttuun ympäristöön. Kuitenkin jatkossa, jos etäkäyttöyhteyden nopeutta haluttaisiin parantaa, voidaan USB-verkkosovittimen tilalta käyttää muihin dataväyliin tarkoitettuja verkkokorttimalleja. USB-2.0:n teoreettinen maksiminopeus on 480Mbit/s, joka on melko hidas, mutta kuitenkin kyseiseen käyttöön riittävä, sillä verkkoyhteyden nopeus tietokoneiden välillä oli käytetyllä verkkolaitteistolla 100Mbit/s. USB-verkkosovittimen etuna on pidettävä helppoa asennettavuutta ja siirrettävyyttä, sillä verkkoyhteys voidaan muodostaa ja purkaa nopeasti ilman mitään pysyviä asennuksia tai muutoksia tietokoneen laitteiston kokoonpanoon. Tarkasteltaessa muita mahdollisia verkkoympäristön toteutusmalleja todettiin, että ne olisivat mahdollisia toteutuksensa puolesta, mutta vaatisivat mittavampia muutoksia laitteistoon sekä erityisesti palvelinkoneen ohjelmistoihin ja verkkoasetuksiin.

Palomuuriasetukset toteutettiin siten, että liikenne etätyöpöytäyhteyksien käyttämiin portteihin oli sallittua palvelinkoneella. Tämän tyyppisessä verkkoympäristössä palomuuri voidaan poistaa palvelinkoneen osalta pois käytöstä, mutta tällöin on tiedostettava tämän toimenpiteen aiheuttamat riskit. Päätekoneen palomuuriasetuksiin ei puututtu.

Vertailtaessa etätyöpöytäohjelmistoja ei havaittu mitään mullistavia eroja suoritusnopeudessa tai käytettävyydessä. Merkittävimmät erot ohjelmistoissa olivat turvallisuuden toteutuksessa. Vaikka ohjelmistojen turvallisuudessa on eroja ja siihen kiinnitettiin huomiota tätä työtä tehtäessä, ei se muodostu kyseisessä verkkoympäristössä ratkaisevaksi tekijäksi. Etäyhteysverkko on erillään muusta julkisesta verkosta fyysisesti omassa tilassaan ja johon ei verkkoyhteyden kautta päästä ulkopuolelta, lisäksi palvelinkone ei sisällä mitään salassa pidettävää tietoa tai ohjelmistoja, joiden käyttöä pitäisi rajoittaa.

Testattaessa etätyöpöytäyhteyttä päätekoneelta järjestelmänvalvojan käyttöoikeuksien lisäksi myös niin sanottuna peruskäyttäjänä eli tässä tapauksessa opiskelijana, jonka järjestelmän käyttöoikeudet ovat rajattuja, törmättiin Windows etätyöpöytäyhteyden käytössä samaan ongelmaan kuin aiemmin. Päätekoneiden molempien verkkokorttien ollessa aktiivisessa tilassa (enabled), Windowsin etätyöpöytä ei havainnut palvelinkonetta etäkäyttöverkossa ja yhteyden muodostus epäonnistui. Rajatut käyttöoikeudet eivät mahdollistaneet päätekoneen verkkoasetusten muuttamista, jotta varsinainen verkkokortti olisi yhteyden muodostuksen ajaksi voitu sulkea. Muilla testatuilla ohjelmistoilla eli TightVNC:llä ja TeamViewerillä ei kyseistä ongelmaa havaittu vaan etätyöpöytäyhteyden muodostus onnistui rajatuillakin käyttöoikeuksilla. Mikäli yhteyttä käytetään päätekoneelta muilla, kuin järjestelmänvalvojan oikeuksilla, suositellaankin käytettäväksi joko TightVNC:tä tai TeamVieweri:ä. Ohjelmistojen turvallisuuden vertailussa TightVNC:n ja TeamViewerin välillä, todettiin TeamViewerin olevan näistä kahdesta turvallisempi etätyöpöytäohjelmisto.

7.2 Jatkokehitys

Toteutettu verkkoympäristö täyttää sille ennalta määritetyt vaatimukset ja testatut ohjelmistot mahdollistivat yhteyden muodostuksen etäyhteysverkon laitteiden välille. Varsinaisesti kyseiseen toteutusmallin jatkokehitystarpeita ei ilmennyt. Yhtenä kehityskohteena olisi muiden lähiverkkotekniikoiden käyttö etäyhteyden muodostuksessa, esimerkkinä mainittakoon WLAN. Lisäksi voitaisiin tarkastella, onko olemassa muita menetelmiä tämän tyyppisen etäkäyttöympäristön toteuttamiseksi.

Etätyöpöytäohjelmistojen käytön kannalta jatkossa haasteena on verkkoympäristön toteutus siten, että Windows etätyöpöytää käytettäessä päätekoneen verkkoasetuksiin ei tarvitsisi puuttua yhteydenmuodostuksessa palvelinkoneelle.

8 YHTEENVETO

Työn tavoitteena oli suunnitella ja toteuttaa etäkäyttöympäristö, jossa kahdella tietokoneella voitaisiin työskennellä samanaikaisesti etätyöpöytäyhteyden kautta. Etäyhteys oli tarkoitus toteuttaa siten, että se olisi mahdollisimman turvallinen ja helppokäyttöinen.

Kirjallisessa osassa käsiteltiin etäkäyttöä ja siihen liittyviä protokollia, lähiverkkoympäristöjen taustoja ja etäkäytön tietoturvallisuutta, kuten erilaisia salausmenetelmiä sekä etäkäyttöön liittyviä uhkakuvia. Etäkäyttöprotokollista tarkasteltiin kaksi ainakin Windows ympäristöissä yleisintä protokollaa eli RDP ja RFB. Lähiverkkoja tarkasteltaessa käsiteltiin TCP/IP-viitekehystä ja OSI-mallia, sekä Ethernetiä, joka on yleisin lähiverkkotekniikka.

Varsinaisena tavoitteena tälle työlle oli verkkoyhteyden muodostus päätekoneen ja etäkäytettävän koneen välille, josta tässä dokumentissa käytetään nimitystä palvelinkone. Lisäksi etäkäyttöverkossa olevien laitteiden verkko- ja palomuuriasetukset tuli mukauttaa, siten että turvallisuus ja käytettävyys olisivat mahdollisimman hyvällä tasolla. Verkkoympäristö toteutettiin lisäämällä päätekoneeseen toinen verkkosovitin ja kytkemällä palvelinkone tähän verkkosovittimeen ristiinkytketyn CAT5-verkkokaapelin kautta. Lisäksi testattiin verkkoratkaisua, jossa yhteys muodostettaisiin laitteiden välille verkkokytkimen kautta, tämän ratkaisumallin todettiin olevan mahdollinen, mutta tähän tarkoitukseen kuitenkin sopimaton. Verkkoasetuksista määriteltiin etäyhteysverkon verkkosovittimille kiinteät IPv4-osoitteet. Palomuuriasetuksiin ei päätekonen osalta puututtu lainkaan, sillä kyseinen tietokone on varsinaisen verkkosovittimensa välityksellä yhteydessä myös ulkopuoliseen verkkoon. Palvelinkoneen asetuksista sallittiin etätyöpöytäyhteyden muodostus kyseiselle koneelle ja palomuuriasetuksista sallittiin yhteydet etätyöpöytäohjelmistojen käyttämiin TCP-portteihin.

Verkkoyhteyden muodostuksen, sekä palomuuri- ja verkkoasetusten mukauttamisen lisäksi testattiin ja vertailtiin kolmea etätyöpöytäohjelmistoa, jotka olivat Windows etätyöpöytä, TightVNC ja TeamViewer. Ohjelmistojen peruskäytössä ja ominaisuuksissa ei havaittu suurta eroa niitä testattaessa. Ongelmia aiheutti lähinnä Windows etätyöpöydän yhteydenmuodostus, jolloin ohjelmisto ei havainnut palvelinkonetta etäyhteysverkossa. Etätyöpöytäyhteyden muodostamiseksi Windowsin etätyöpöydällä, tuli päätekoneen toinen verkkosovitin sulkea yhteydenmuodostuksen ajaksi.

Työn tuloksena saatiin toimiva etäkäyttöympäristö, joka mahdollisti palvelinkoneen käytön etätyöpöydän kautta. Ohjelmistotestauksessa ei havaittu merkittäviä eroja ohjelmistojen välillä, mutta johtuen ongelmista Windows etätyöpöydän yhteyden muodostuksessa, käytettäväksi ohjelmistoksi suositellaan, joko TightVNC:tä tai TeamViewer:iä.

LÄHTEET

1 Kajaanin ammattikorkeakoulu. Toiminta. Viitattu 22.3.2012. [WWW-sivusto]

http://www.kajak.fi/suomeksi/Esittely/Toiminta.iw3

2 TechTarget. Remote Desktop Definition. Viitattu 27.2.2012. [WWW-sivusto]

http://searchenterprisedesktop.techtarget.com/definition/remote-desktop

3 VAHTI, Valtionhallinnon tietoturvallisuuden johtoryhmä. Turvallinen etäkäyttö turvattomissa verkoissa. 2003. 83 s. [PDF-dokumentti]. ISBN 951-804-395-7.

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/44981/44978_fi.pdf.

4 Microsoft. Remote Desktop Protocol. Päivitetty 7.9.2011. [WWW-dokumentti]

http://msdn.microsoft.com/en-us/library/aa383015(v=VS.85).aspx

5 Microsoft. [MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Specification. Päivitetty 16.12.2011. [PDF-dokumentti]

http://msdn.microsoft.com/en-us/library/cc240445(PROT.10).aspx

6 Richardson, T. The RFB Protocol (Version 3.8). Päivitetty 26.11.2010. [PDF-dokumentti]
http://www.realvnc.com/docs/rfbproto.pdf

7 Granlund, K. Tietoliikenne. 1., painos. Porvoo: WS Bookwell, 2007. 448 s. ISBN 978-951-0-32821-7.

8 Hakala, M., Vainio, M., Vuorinen, O. Tietoturvallisuuden käsikirja. 1., painos. Porvoo: WS Bookwell, 2006. 421 s. ISBN 951-846-273-9.

9 Paananen, J. Tietotekniikan peruskirja. 1., painos. Porvoo: WS bookwell, 2005. 483 s. ISBN 951-846-250-X

10 Jaakohuhta, H. Lähiverkot-Ethernet. Jyväskylä: Gummerus Kirjapaino Oy, 2000. 322 s. ISBN 951-826-013-3.

11 Raahen tekniikan ja talouden yksikkö. Lähiverkot. Viitattu 27.2.2012. [WWW-sivusto]

http://www.ratol.fi/opensource/lahiverkot/index.htm

12 Ruohonen, M. Tietoturva. Porvoo: WS Bookwell, 2002. ISBN 951-846-163-5.

13 CERT-FI. Haavoittuvuustiedote 011/2012, Symantec pcAnywhere –ohjelmistojen haavoittuvuuksia korjattu. Julkaistu 25.1.2012. [WWW-dokumentti] http://www.cert.fi/haavoittuvuudet/2012/haavoittuvuus-2012-011.html

14 CERT-FI. Tietoturva nyt! Haittaohjelma Morto leviää Remote Desktop –etähallinnan kautta. Päivitetty 29.8.2011. [WWW-dokumentti]

http://www.cert.fi/tietoturvanyt/2011/08/ttn201108291605.html

15 Viestintävirasto. Salausmenetelmät. Viitattu 27.2.2012. [WWW-sivusto]

http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html

16 Stallings, W. Cryptography and Network Security. Principles and Practices. 3., kansainvälinen painos. New Jersey, USA: Pearson Education Inc., 2003. 649 s. ISBN 0-13-111502-2.

17 Krutz, R-L, Vines, R-D, Suominen, E(suom.). Tietoturvasertifikaatti – CISSP. Helsinki: Edita Prima Oy, 2003. 543 s. ISBN 951-826-657-3.

18 Rekhter, Y, Moskowitz, B, Karrenberg, D, de Groot, G.J, Lear, E. Address Allocation for Private Internets. Julkaistu Helmikuussa 1996. [PDF-dokumentti]

http://tools.ietf.org/pdf/rfc1918.pdf

19 Microsoft, Technet. Windows Firewall. Päivitetty 14.4.2011. [WWW-dokumentti] http://technet.microsoft.com/en-us/network/bb545423

20 Richardson, T, Levine, J, (IETF). The Remote Framebuffer Protocol. Julkaistu marraskuussa 2011. ISSN: 2070-1721. [TXT-dokumentti]

http://tools.ietf.org/rfc/rfc6143.txt

21 Wikipedia(en). Remote Desktop Services. Päivitetty 31.3.2012. [WWW-dokumentti]

http://en.wikipedia.org/wiki/Remote_Desktop_Services

22 TightVNC. TightVNC-ohjelmiston kotisivu. Viitattu 22.3.2012. [WWW-sivusto] http://www.tightvnc.com/

23 TeamViewer. Ohjelmiston lataussivusto. Viitattu 22.3.2012. [WWW-sivusto] http://www.teamviewer.com/fi/download/index.aspx

24 TightVNC. Frequently Asked Questions. Viitattu 22.3.2012. [WWW-sivusto] http://www.tightvnc.com/faq.php