ETÄTYÖPÖYTÄYHTEYKSIEN TESTAUS

Hannula

Toni

2009 Laurea Leppävaara

Toni Hannula

ETÄTYÖPÖYTÄYHTEYKSIEN TESTAUS

ETÄTYÖPÖYTÄYHTEYKSIEN TESTAUS

Toni Hannula
Opinnäytetyö
Syksy 2009
Tietojenkäsittelyn koulutusohjelma
Laurea ammattikorkeakoulu

Toni Hannula. Etätyöpöytäyhteyksien testaus. Espoo 2009. Laurea ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma, yritysten tietoverkot, tradenomi. Opinnäytetyö 40 sivua + 6 sivua liitteitä.

TIIVISTELMÄ

Opinnäytetyössä tutkittiin eri etäkäyttöohjelmia ja vertailtiin niiden mahdollisuuksia toimia lähiverkossa Windows-ympäristön ylläpidossa. Vertailun tekeminen oli tärkeää, koska vastaavanlaista vertailua ei ollut aikaisemmin tehty kyseiselle yritykselle. Etäkäyttöohjelmia oli tarjolla erittäin paljon ja ne olivat hyvin eritasoisia.

Vertailtavaksi otettiin ilmaisia ja maksullisia etäkäyttöohjelmia. Se sisälsi seuraavat ohjelmat Etätyöpöytäyhteys, NetOp Remote Control, RealVNC, TeamViewer, TightVNC ja UltraVNC. Ohjelmien testaus tapahtui yhden tietokoneen avulla, mihin asennettiin virtuaaliset Windows XP ja 2000 –käyttöjärjestelmät. Virtuaaliset käyttöjärjestelmät toimivat ohjelmien vertailussa etäkäyttöohjelmistojen asiakasohjelman käyttöjärjestelmänä.

Vertailun tulosten perusteella NetOp Remote Control osoittautui parhaaksi vaihtoehdoksi maksullisista ohjelmista. UltraVNC puolestaan oli paras vaihtoehto ilmaisista ohjelmista. Työn tuloksena syntyi vertailu etäkäyttöohjelmista ja hankintaehdotus.

Asiasanat: etäkäyttö, thin client, palvelintekniikka, VNC, RDP, DTL

SUMMARY

The thesis consists of comparing various remote access programs and testing their possibilities to function in local area network and Windows environment administration. The comparison was important since the company had not done similar one before. There were multiple remote desktop programs to choose from and the quality of them was alternating.

In the comparison were free and chargeable programs. The programs were Windows Remote Desktop, NetOp Remote Control, RealVNC, TeamViewer, TightVNC and UltraVNC. The testing of the programs was done with the help of one computer which had Windows XP and 2000 operating systems installed in it virtually. Virtual operating systems functioned as the client software's operating system.

The results indicated that the most suitable program from the chargeable category was NetOp Remote Control. UltraVNC on the other hand was the best option from the free category. As the result of the thesis a comparison of remote access programs and a proposal of procurement was formed.

SISÄLLYS

1 JOHDANTO

Tämä opinnäytetyö on tehty Helsingissä sijaitsevalle Yritys X:lle. Työn tarkoituksena oli vertailla etäkäyttöohjelmia ja tehdä parhaiten toimeksiantajalle soveltuvasta ohjelmasta hankintaehdotus. Etäkäyttöohjelmien välillä vertailtiin toteutettua asennettavuutta, käytettävyyttä, tietoturvaa, verkonkäyttöä ja hintaa. Työ tehtiin erittäin tiiviissä yhteistyössä yrityksen it-vastaavan henkilön kanssa.

X Yhtiöiden omistama Yritys X on vuonna 1957 perustettu perheyritys, joka lukeutuu tänä päivänä Suomen suurimpiin ja monipuolisimpiin kopio- ja painopalveluiden tuottajiin. Yhtiön hallinnoimat yritykset Yritys X, Yritys X Finland Oy sekä Viron alueella toimiva osakkuusyritys Yritys X Oy ovat kukin omina yksikköinään ja omilla toimialueillaan palvelevia tuotantoyhtiöitä.

Toimintaympäristö koostuu työasemista, joissa on käyttöjärjestelmänä Windows XP tai 2000. Tietokoneet on jaettu kahteen erilliseen verkkoon. Käyttäjäverkko on tarkoitettu työkäyttöön ja hallinnon verkko hallinnolliseen käyttöön. Työn tarkoituksena on saada toimeksiantajalle toimiva etäkäyttöohjelmisto hallinnon verkkoon, joka koostuu noin sadasta hallinnon ja kolmesta atk-tuen työasemasta. Tukipyynnöt toimeksiantajalla tapahtuvat yleensä puhelimitse tai sähköpostitse.

Opinnäytetyön myötä tarjoutuu atk-tuelle mahdollisuus ratkaista tukipyyntöjä ilman fyysistä paikallaoloa apua tarvitsevalla työpisteellä. Tämä nopeuttaa ja helpottaa atk-tuen tukipyyntöjen käsittelyä ja vähentää liikkumista työpisteiden välillä.

Opinnäytetyön luonnetta voi kuvailla empiirisenä selvityksenä. Opinnäytetyö on rajattu etäkäyttöohjelmien teknisiin ja ohjelmallisiin toimivuuksiin. Näin työn teoriaosa koostuu verkkoarkkitehtuurien, etäkäytön protokollien ja tietoturvan esittelystä.

2 PALVELINTEKNIIKKA

Palvelintekniikka (client-server architecture) on tietojenkäsittelyjärjestelmän toimintaperiaate, jossa tehtävän suoritus on jaettu käyttäjän työaseman ja eri osatehtäviin erikoistuneiden palvelimien kesken (Tietotekniikan liitto). Laitteiston lisäksi tilanteesta riippuen palvelintekniikka termillä voidaan tarkoittaa tietojenkäsittelytehtävien jakamista usealle ohjelmalle (Lamminmäki S. & Hannus, J.). Arkkitehtuurivaihtoehdot voidaan karkeasti jakaa ohut ja raskas asiakas -malliin sen mukaan, mihin järjestelmän perusyksikköön kohdistuu sovellusten suoritustaakka.

Olennaista palvelintekniikassa on, että tilannekohtaisesti haetaan tehokas työnjako palvelua käyttävän prosessin tai laitteiston ja palvelimen välillä. Eri tilanteet ja sovellusalueet edellyttävät erilaista työnjakoa. (Lamminmäki S. & Hannus, J.)

Palvelintekniikassa ei ole kyse yhdestä ainoasta oikeasta tavasta rakentaa järjestelmiä, vaan käyttöliittymiä, tiedonhallintaa ja sovelluslogiikkaa voidaan jakaa monella eri tavalla työasemien ja palvelimien välille. Näistä mahdollisuuksista syntyy useampi arkkitehtuurivaihtoehto. (Lamminmäki S. & Hannus, J.)

2.1 Ohut asiakas

Ohut asiakas (thin client) -mallin lähtökohta on, että palvelin suorittaa suurimman osan prosesseista ja asiakas hoitaa ohjauksen ja kuvan vastaanottamisen. Voidaan siis sanoa, että ohut asiakas –malli on hyvin palvelinkeskeinen. Palvelinkeskeisyys mahdollistaa palvelimen sovellusten käyttämisen asiakkaan laitteistosta, ohjelmistosta ja yhteydestä riippumatta. Ohut asiakas -malli voidaan toteuttaa joko laitteisto- tai ohjelmistopohjaisesti. (Kanter)

Laitteiston avulla toteutetulla ohut asiakas -mallilla viitataan asiakaspään tietokoneeseen, jota kutsutaan ohut asiakas -päätelaitteeksi. Päätelaitteet ovat rakenteeltaan yksinkertaisempia ja suorituskyvyltään heikompia kuin nykypäivän pöytätietokoneet. Niiden rakenteesta ja suorituskyvystä pystytään tinkimään, koska kaikki laskenta tapahtuu palvelinpäässä. Käyttäjältä vaaditaankin ainoastaan hiiri, näppäimistö, näyttö ja itse ohut asiakas -päätelaite. Päätelaitteen tehtävänä on muodostaa yhteys ja kommunikoida palvelimen kanssa sekä suorittaa yksinkertaisia käskyjä. Käyttäjälle voidaan lisäksi tarjota mahdollisuus käyttää ulkoista muistia. (Taimila 2007)

Ohjelmiston avulla toteutettu Ohut asiakas -malli on hyvin samanlainen kuin laitteiston avulla toteutettu. Suurimpana erona on, että yhteyden muodostus ja kommunikointi palvelimen

kanssa sekä yksinkertaisten käskyjen suorittaminen tapahtuu erillisen ohjelman avulla. Nämä erilliset ohjelmat sisältävät yleensä ainoastaan käyttöliittymän esittämiseen tarvittavat komponentit. (Taimila 2007)

2.2 Raskas asiakas

Raskas asiakas (fat client, rich client) -malli on vastakohta ohut asiakas -mallille. Laitteiston näkökulmasta raskas asiakas –päätelaite on tietokone, johon on asennettu käyttöjärjestelmä ja merkittävä osa tarvittavista ohjelmista. Koska raskas asiakas –päätelaite ei hyödynnä palvelimen suorituskykyä, sen tarvitsee olla suorituskyvyltään tehokkaampi tietokone kuin vastaavaan tarkoitukseen käytettävä ohut asiakas –päätelaite. (Sanastokeskus TSK 2000)

Työpöytäkoneiden suorituskyvyn räjähdysmäisen kasvun tuloksena nykypäivän kouluissa ja työpaikoilla ylivoimaisesti yleisin ratkaisu on raskas asiakas –järjestelmä, jossa sovelluksia ajetaan työasemakohtaisesti. Tämä ratkaisu asettaa kuitenkin resurssi ja kustannuspaineita ylläpitoon. Raskaan asiakas –mallin heikkoudet havaittiin jo, kun aloitettiin yksittäisten työasemien ylläpito. Ylläpitoa varten täytyi palkata lisää henkilökuntaa. Käyttöjärjestelmien alttius tietokoneviruksille ja peruskäyttäjän tietoturvan tietotaidon puute kohdisti uusia vaaroja tietojärjestelmiin. Mallin perusongelmana onkin tietoturva sekä yhteisten resurssien jakaminen. Tämän lisäksi vielä on huolehdittava jokaisen työaseman ylläpidosta. (SearchWinIT.com)

3 ETÄKÄYTÖN PROTOKOLLAT

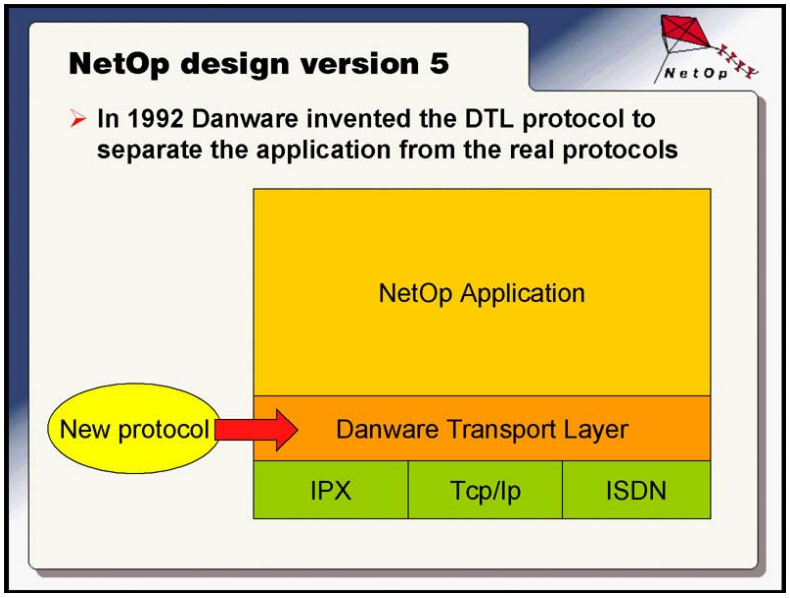
Protokolla eli yhteyskäytäntö on sovittu tapa tai kokoelma sovittuja tapoja, joiden avulla tietokoneet voivat keskustella tietoverkkojen yli. Protokollien olemassaolo mahdollistaa eri valmistajien tekemien laitteiden keskustelun keskenään. Tietoliikenteessä protokollat määrittelevät pääasiassa viestin muodon, ajoituksen, jaksotuksen ja virheenkorjauksen. (Tietotekniikan liitto ry)

Tietoliikenneprotokollia määrittelevät useat standardointielimet, kuten IEEE (Institute of Eletrical and Eletronic Engineers), ANSI (American National Standards Institute), TIA (Telecommunications Industry Association), EIA (Eletronic Industries Alliance) ja ITU (International Telecommunications Union).
(Ciscon verkkoakatemia)

Etäkäyttöohjelmien käyttämiä protokollia on useita erilaisia. Protokollat tarjoavat etäkäyttöohjelmille säännöt yhteyden muodostamiselle ja kommunikoinnille. Etäkäyttöön ei ole suunniteltu vakiintunutta protokollaa, vaan jokaiselle ohjelmalle on ohjelman valmistaja kehittänyt omanlaisen protokollan. Tässä kappaleessa kerrotaan vertailtavien etäkäyttöohjelmien käyttämistä protokollista. DTL (Danware Transport Layer) on maksullisen NetOp RC -etäkäyttöohjelmiston käyttämä protokolla. RFB (Remote Framebuffer) on vapaa protokolla, johon pohjautuvat kaikki VNC -etäkäyttöohjelmat. Viimeisenä on RDP (Remote Desktop Protocol) –protokolla, jota käytetään Windowsin etätyöpöytäyhteys sovelluksessa.

3.1 Danware Transport Layer

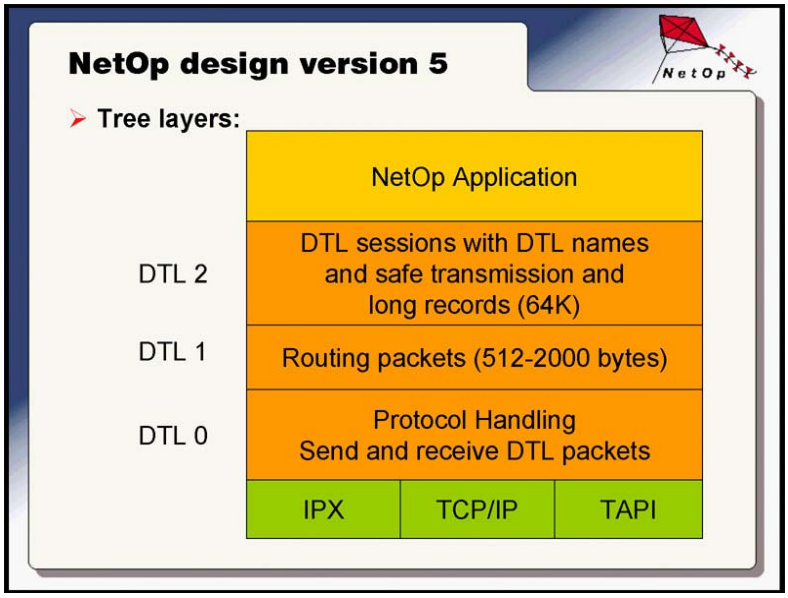
DTL (Danware Transport Layer) on Danware A/S:n vuonna 1992 kehittämä kuljetuskerroksen protokolla. Kehitys sai alkunsa, kun oli kallista ja aikaa vievää kirjoittaa ohjelma tai ohjelman osa jokaiselle tiedonsiirto protokollalle ja käyttöjärjestelmälle. Saadakseen kattavasti toimivan etäkäyttöohjelman, Danware kehitti protokollan, joka erottaa ohjelmatason standardoiduista tiedonsiirron protokollista (kuvio 1). Tällä luotiin tuki nykyisille ja tuleville tiedonsiirron protokollille, sekä useille käyttöjärjestelmille. Tiedonsiirron lisäksi DTL -protokollan tehtävänä oli hoitaa tiedon turvallinen välitys, asiakasohjelmien nimeäminen sekä DTL -pakettien reititys, lähetys ja vastaanotto. (Jukka Stenius)



KUVIO 1. DTL -protokollan sijoittuminen (Jukka Stenius)

DTL -verkossa jokaisella asiakkaalla ja palvelimella tulee olla DTL -nimike. DTL -verkko on jaettu aliverkkoihin, jotka muodostuvat eri kuljetusprotokollista.
Kuljetuskerroksen protokollat on jaettu kahteen eri ryhmään; dynaamisiin joihin luetaan: ISDN, TAPI, Serial, APPC ja TCP ja staattisiin joita on IPX, NetBIOS ja UDP. (Jukka Stenius)

DTL -protokollassa on käytössä kolme kerrosta normaalin OSI -mallin esitystapa- ja istuntokerroksen sijaan. Ylin kerros (DTL 2) hoitaa DTL -protokollan istuntoja nimikkeiden kanssa, turvallisen tiedonvälityksen ja ohjelman lähetettävien ja vastaanotettavien tietojen käsittelyn. DTL 1 -kerros huolehtii ohjelman tietopakettien reititystiedoista ja reitityksestä. DTL 0 hoitaa DTL pakettien lähettämisen ja keskustelun eri protokollien kanssa. (Jukka Stenius) Kuviossa 2 on kuvattuna DTL –protokollan eri kerrokset.



KUVIO 2. DTL -protokollan kerrokset. (Jukka Stenius)

3.2 Remote Desktop Protocol

RDP (Remote Desktop Protocol) on Microsoftin kehittämä kuljetuskerroksen protokolla. RDP tarjoaa joustavan alustan ja tuen yli 64 000 erilaiselle kanavalle tiedonsiirtoon ja ehdot monipistetiedonsiirtoon. Kuljetuskerros kuuluu ja on osa avointa ITU T.120 protokollastandardi perhettä. Monikanavaisuuden johdosta RDP toimii vain Windows 2000,

2003 ja XP -käyttöjärjestelmäympäristössä, mutta on suunniteltu tukemaan erilaisia verkkotopologioita ja useita lähiverkon protokollia. (MSDN, 2007)

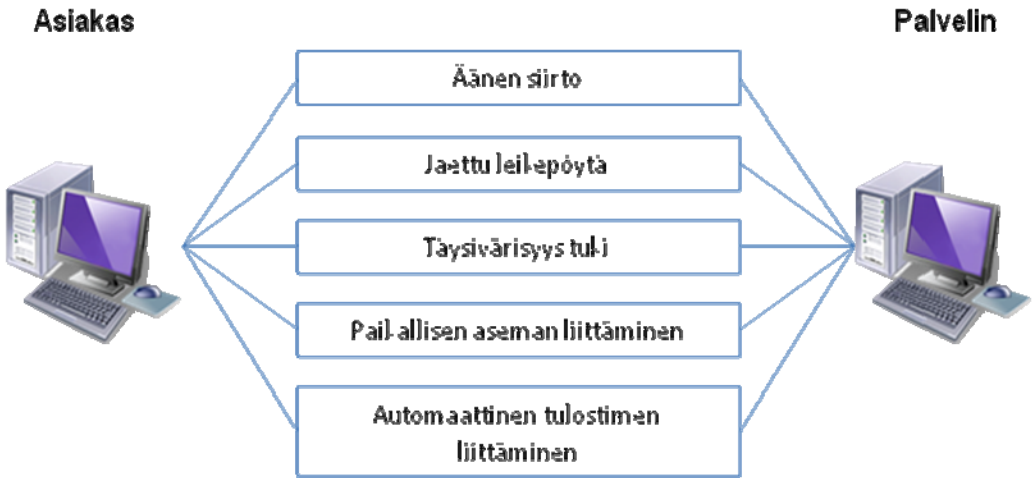
RDP palvelin käyttää palvelimen omaa videoajuria näytettävän kuvan renderöimiseen. Tämän jälkeen renderöity tieto pakataan verkkopaketeiksi ja lähetetään verkon läpi asiakkaalle käyttämällä RDP kuljetuskerrosta. Asiakas vastaanottaa renderöidyn tiedon ja tulkitsee verkkopaketit Microsoft Win32 GDI API kutsuiksi. (MSDN, 2007)

Turhan tiedon lataamisen välttämiseksi asiakas käyttää client-side caching –toimintoa, joka mahdollistaa istunnon aikana ladattujen kuvien muistamisen. Toiminnon avulla asiakas lataa palvelimelta ainoastaan ne kuvat, jotka ovat päivittyneet. Ladattu tieto varastoidaan kiintolevyn välimuistiin ja lopulta poistetaan käyttäen LRU (Least Recently Used) –algoritmia. Kiintolevyn välimuistin täyttyessä algoritmi poistaa tiedon joka on ollut käyttämättömänä pisimpään. (Minasi ym.)

Näppäimistön ja hiiren tapahtumat puolestaan välitetään asiakkaalta suoraan palvelimelle. Tapahtumien vastaanottamiseen palvelin käyttää näppäimistön ja hiiren ajuria, jotka on asennettu palvelin koneelle. (MSDN, 2007)

RDP kuljetuskerros on erilaisten kanavien kokoelma. Kanavien tehtävänä on siirtää tietoa asiakkaan ja palvelimen välillä. Ne määrittävät, myös etäkäyttöistunnon aikana seuraavia asioita: miltä istunto näyttää ja kuinka yksittäinen sovellus on vuorovaikutuksessa asiakaspäätelaitteeseen. Toimiakseen kanavan täytyy olla avoimena sekä asiakkaalla että palvelimella. (Minasi ym. 2003)

Jokaisen protokollaversion ominaisuudet riippuvat kanavien lukumäärästä. Protokollaversion kasvaessa kasvaa myös kanavien lukumäärä ja tarvittava kaistanleveys. Kanavien täytyy olla avoimena palvelimella ja asiakkaalla, että niitä voidaan käyttää. RDP kuljetuskerros sisältää seuraavia kanavakokonaisuuksia (kuvio 3): Äänen siirto (Sound transfer), Jaettu leikepöytä (Shared clipboard), Täysvärisyydentuki (True Color support), Paikallisen aseman liittäminen (Local drive mapping) ja Automaattinen tulostimen liittäminen (Automatic printer mapping). (Minasi ym)

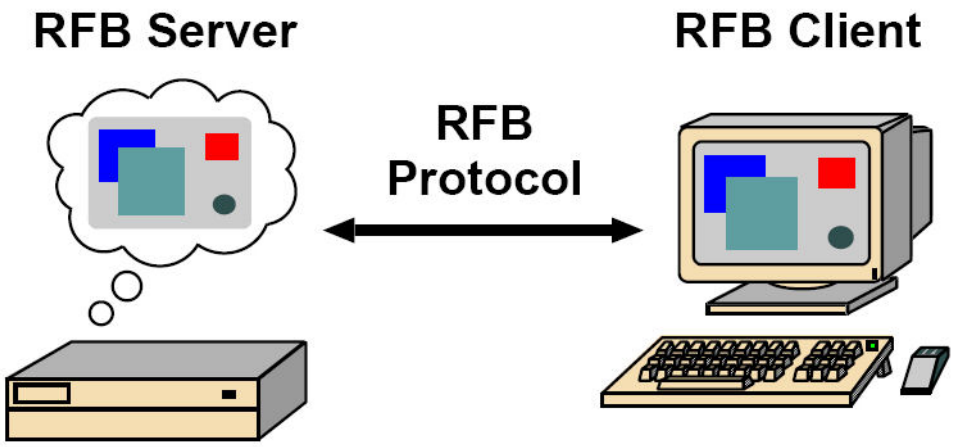


KUVIO 3. RDP kuljetuskerroksen kanavointi. (Minasi ym)

3.3 Remote Framebuffer

Ohut asiakas -malliin pohjautuva RFB –protokolla (Remote Framebuffer) soveltuu kaikille käyttö- ja ikkunointijärjestelmille. RFB –protokolla asettaa hyvin vähäiset vaatimukset asiakastietokoneelle ja verkkoyhteydelle. Tämä tarjoaa asiakkaalle mahdollisuuden muodostaa yhteys palvelimeen paikasta riippumatta. (RealVNC 2002, viitattu 23.09.2007.) RFB –protokollasta käytetään myös nimitystä VNC (Virtual Network Computing) –protokolla. (RealVNC)

RFB palvelin suorittaa kaikki prosessit ja laskennat, mikä vähentää ylimääräistä verkkoliikennettä ja keventää RFB asiakkaiden toimintaa. Niiden tehtäväksi jääkin näin vain etäyhteyden avaaminen, palvelimen operoiminen ja kuvan piirtäminen käyttäjälle (kuvio 4). (RealVNC 2002)



KUVIO 4. RFB Palvelin – Asiakas toiminta. (RealVNC 2002)

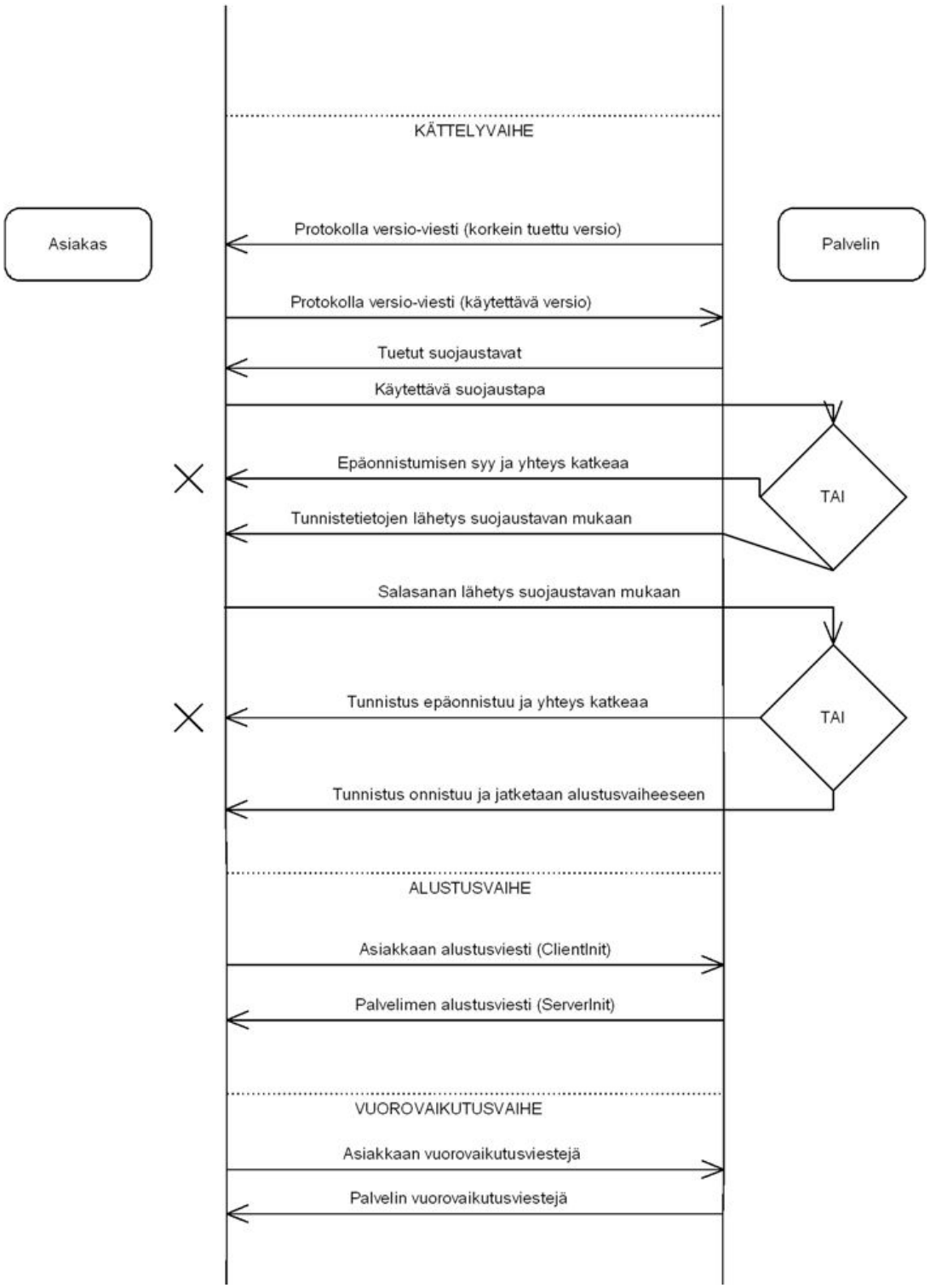
RFB voidaan jakaa näyttö (display) ja syöttö (input) protokollaan. Näyttöprotokolla piirtää pikselitiedon muodostaman suorakaiteen annettuun paikkaan näytöllä. Pikselitiedon päivitysten sarjaa kutsutaan kuvan puskurimuistin päivitykseksi. Päivitys esittää kuvan puskurimuistin tilan muutoksen. Jossain määrin tämä esitystapa on samanlainen kuin videon yksittäisessä kuvassa. Päivitys tapahtuu ainoastaan asiakkaan pyynnöstä. Tästä syystä, mitä hitaampi asiakas ja verkko ovat, sitä hitaammin päivityksiä asiakkaalle tulee. (RealVNC 2002)

Syöttöprotokollan tehtävänä on lukea asiakkaan suorittamat syöttötapahtumat ja lähettää ne palvelimelle. Syöttötapahtumiin luetaan näppäimistön, hiiren sekä standardoimattomien I/O-laitteiden tapahtumat. Standardoimattomilla I/O-laitteilla tarkoitetaan esimerkiksi digitaalista kynää, jonka liikkeet voidaan kääntää näppäimistön tai hiiren liiketapahtumiksi. (RealVNC 2002)

Protokollaa on mahdollista laajentaa kolmella eri tavalla: koodaustavalla (encoding), näennäiskoodauksella (pseudo encoding) ja turvallisuustavalla (security type). Koodaustavalla tarkoitetaan tapaa, jolla pikselitiedot lähetetään palvelimelta asiakkaalle. Näennäiskoodausta käytetään kursorin liikkeen ja työpöydän muodostamiseen. Turvallisuustavat puolestaan liittyvät käyttäjän varmentamiseen. (RealVNC 2002)

RFB -protokollan viestintä jaetaan kolmeen eri vaiheeseen (kuvio 5). Ensimmäisessä vaiheessa sovitaan käytettävästä protokollaversiosta ja turvallisuustavasta. Tämän jälkeen turvallisuustavasta riippuen suoritetaan asiakkaan tunnistus. Tätä vaihetta kutsutaan kättelyvaiheeksi (handshaking phase). Kättelyvaiheen jälkeen aloitetaan alustamisvaihe

(Initialisation phase), jossa asiakas ja palvelin vaihtavat ClientInit ja ServerInit -viestejä. Viestinnän viimeinen vaihe on palvelimen ja asiakkaan välillä tapahtuvaa vuorovaikutusta. (RealVNC 2002)



KUVIO 5. RFB –protokollan vuorovaikutus

Kättelyvaihe alkaa, kun palvelin lähettää asiakkaalle *ProtocolVersion* –viestin. Viestistä käy ilmi palvelimen korkein tuettu RFB -protokollaversio. Tällä hetkellä ainoat julkaistut protokollaversiot ovat 3.3, 3.7 ja 3.8. Asiakas vastaa *ProtocolVersion* –viestillä, mitä protokollaversiota tulisi käyttää. Asiakkaan ei tule koskaan pyytää korkeampaa protokollaversioita kuin palvelimen ilmoittama. Tällä taataan, että asiakkaat ja palvelimet ovat alaspäin yhteensopivia. Protokollaversion sopimisen jälkeen, palvelin ja asiakas sopivat käytettävästä turvallisuustavasta ja palvelin yrittää tunnistaa asiakkaan. Tunnistuksen jälkeen palvelin sallii tai sulkee yhteyden. Uusien koodauksien lisäys tai näennäiskoodauksen lisääminen ei vaadi protokollaversionumeron muuttamista, koska palvelin hylkää koodaukset, joita se ei ymmärrä. (RealVNC 2002)

Käytettävän turvallisuustavan sopimisessa on pieniä eroja versiosta riippuen. RFB 3.3 versiossa palvelin päättää turvallisuustavan ja lähettää asiakkaalle ilmoituksen käytettävästä turvallisuustavasta. *Security-type -viesti* voi sisältää ainoastaan jonkin seuraavista arvoista 0, 1 tai 2. Arvo 0 tarkoittaa yhteyden epäonnistumista. Arvo 1 tarkoittaa, ettei oteta turvallisuustapaa käyttöön. Arvo 2 tarkoittaa, että käytetään VNC -tunnistusta (VNC Authentication) turvallisuustapana. VNC -tunnistuksessa palvelin lähettää asiakkaalle satunnaisen 16-tavuisen haasteen (challenge). Asiakas vastaa salaamalla haasteen DES -salauksella, käyttäen avaimena käyttäjän antamaa salasanaa. Asiakkaan salaamasta viestistä muodostuu 16-tavuinen vastaus palvelimelle. (RealVNC 2002)

RFB versiosta 3.7 ylöspäin, palvelin lähettää asiakkaalle listan palvelimen tukemista turvallisuustavoista. Asiakkaan tukeman turvallisuustavan löytyessä listalta, asiakas lähettää palvelimelle ilmoituksen käytettävästä turvallisuustavasta. Mikäli palvelimelta asiakkaalle lähettetty lista ei sisällä yhtään turvallisuustapaa, yhteys epäonnistuu. Tämän jälkeen palvelin lähettää asiakkaalle epäonnistumisen syyn ja sulkeen yhteyden. Onnistuneen tunnistuksen jälkeen palvelin lähettää *SecurityResult* -viestin asiakkaalle ja siirtyy alustusvaiheeseen (RealVNC 2002)

Alustusvaiheen viestit

Palvelimen ja asiakkaan läpäistyä kättelyvaiheen, protokolla aloittaa alustusvaiheen. Asiakas lähettää *ClientInit* -viestin, johon palvelin vastaa *ServerInit* -viestillä. *ClientInit* –viestillä sovitaan jaetaanko palvelimen yhteys muiden asiakkaiden kesken. *ServerInit* -viesti kertoo asiakkaalle päivitettävän kuvan korkeuden ja leveyden, pikselin muodon ja työpöytään liittyvän nimen. Pikselin muoto (Pixel_Format) sisältää mm. seuraavia tietoja: pikselin bittien määrän, syvyyden ja väriarvot. (RealVNC 2002)

Vuorovaikutusvaiheen viestit

Alustusvaiheen jälkeen protokolla aloittaa asiakkaan ja palvelimen välisen vuorovaikutuksen. Asiakkaalta palvelimelle välitettäviä vuorovaikutusviestejä ovat: palvelimelta lähetettävien pikseliarvojen muoto, välitettävän kuvan koodaustapa, kuvan päivityspyyntö, näppäimistön ja hiiren toiminnot sekä asiakkaan leikepöytä tekstimuotoisena. Asiakas varmistaa rekisteröimättömien laajennusten tuen palvelimelta, pyytämällä siltä laajennuskohtaisen varmistuksen. Tämä tapahtuu ennen kuin välittää rekisteröimättömän viestin palvelimelle. (RealVNC 2002)

Palvelimelta asiakkaalle välitettäviä rekisteröityjä viestejä ovat kuvan puskurimuistin päivitys, asiakkaan käyttämät värivoimakkuudet, kellonsoitto ja palvelimen leikepöytä tekstimuotoisena. Myös palvelimelta asiakkaalle välitettävissä rekisteröimättömissä viesteissä, on selvitettävä tukeeko asiakas kyseistä laajennusta. Selvitys tapahtuu vastaanottamalla asiakkaalta laajennukseen liittyvä varmistus. (RealVNC 2002)

4 ETÄKÄYTÖN TIETOTURVA

Tietoturva on yksi tärkeä osa etäkäyttöä. Toteutettu tietoturva etätukiohjelmassa on yksi etätukiohjelman laadun mitta. Tietoturva etäkäytössä pitää sisällään käyttäjän tunnistuksen ja etäyhteyden eri tapahtumien salaamisen.

4.1 Käyttäjän tunnistus

Käyttäjän tunnistus eli autentikointi on prosessi, jossa varmennetaan käyttäjä tai identiteetti oikeaksi. Tunnistus tapahtuu kysymällä käyttäjältä salasanaa, turvamerkkiä tai biotunnistetta. Riskin kasvaessa tunnistustavat monimutkaistuvat ja tiukkenevat, jotta voidaan varmistaa käyttäjä turvallisemmin ja varmemmin. (Authenticationworld)

Käyttäjän tunnistus voidaan jakaa kolmeen eri luokaan; salasana, Secure-ID –kortit ja biometriset tunnisteet (Cygate). Salasana tunnistus on yleisin ja turvattomin tunnistustapa. Tämä tunnistustapa vaatii käyttäjää asettamaan käyttäjänimen ja salasanan, jotta kirjautuminen on mahdollista. Erittäin kriittisiä huolenaiheita ovat salasanan pituus, käytettyjen merkkien tyyppi ja salasanan voimassaoloaika. Yleensä pelkkä salasanapohjainen tunnistaminen on vaarallinen, koska käyttäjien salasanat eivät ole aina tarpeeksi monimutkaisia. Lisäksi on olemassa useita erilaisia tapoja saada selville käyttäjien salasanoja. (Authenticationworld)

4.2 Salaus

Salaus ja salaustavat ovat lähtöisin jo ajanlaskumme alkuajoilta, kun keksittiin Atbash-koodi (Tilastokeskus). Tästä lähtien on salauksen tarkoitus ollut varmistaa tietojen luottamuksellisuus, eheys ja kiistämättömyys. Salauksen tavoitteena olisi, että salattua viestiä tai sanomaa ei saisi murrettua kohtuullisessa ajassa ja kohtuullisin resurssein (Viestintävirasto 2006).

Etäkäyttöohjelmien maailmassa salauksen tarkoitus on kuitenkin enemmän vähentää tai estää kokonaan kolmannen osapuolen mahdollisuus päästä hyväksikäyttämään muodostunutta tai muodostuvaa yhteyttä. Etäkäyttöohjelmien käytetyimpiä salausalgoritmeja ovat DES, 3DES, RC4 ja eri avainpituiset AES algoritmit. Maksullisista etäkäyttöohjelmista on mahdollista myös löytää DH76 ja RSA algoritmeja sekä eripituisia tiivistefunktioita.

4.2.1 Symmetrinen salaus

Symmetrisessä salausmenetelmässä käytetään samaa salausavainta viestin salaamiseen ja purkamiseen. Symmetriset salausalgoritmit jaetaan yleisesti jono- ja lohkosalausmenetelmiin. (Viestintävirasto 2006)

Symmetrisen salauksen avainten kokonaistarve on $(n^2 - n)/2$, jossa n on viestijöiden määrä. Jos esim. verkossa on 100 käyttäjää joiden tarvitsee lähettää toisilleen salattuja henkilökohtaisia viestejä, tarvitaan 4950 avainta. (Ståhlberg ja Uskela 1998) Symmetrinen salausmenetelmä sopii ymmärrettävästi parhaiten yhdellä koneella pysyvästi salattavan tiedon salaukseen.

Huonoina puolina menetelmässä on yhden avaimen käyttö. Menetelmän salauksen perustuessa puhtaasti avaimen salaisuuteen, on avainten turvallinen jakaminen erittäin ongelmallista. Symmetrisen salauksen hyvänä puolena on sen nopeus. (Viestintävirasto 2006)

DES (Data Encryption Standard) on symmetrinen lohkosalausalgoritmi. Lohkon pituus on 64 bittiä ja avaimen pituus 56 bittiä. DES on kehitetympi versio 1970 luvun alkupuolella kehitetystä algoritmista nimeltä Lucifer. Nykyisin menetelmää ei pidetä täysin turvallisena, sillä menetelmä pystytään murtamaan alle 24 tunnissa johtuen avainkoon pienuudesta. Menetelmästä kehitettiin myöhemmin 3DES (Triple DES) algoritmi. 3DES menetelmä toimii kuin DES, mutta tieto salataan kolme kertaa. Tämä kasvattaa teoreettisesti avaimen koon 168 bittiin. DES salausta käytetään etäkäyttöohjelmissa käyttäjän tunnistuksessa. (RSA Laboratories)

RC4 (Ron's Code 4) on v.1987 RSA laboratorion Ronald Rivestin kehittämä jonosalaus algoritmi. RC4 on symmetrinen jonosalaaja, sillä se salaa tiedon tavu kerrallaan. Algoritmi perustuu vaihtelevan avainkoon salaiseen avaimeen. Avaimen koko on mahdollista olla jopa 2048 -bittinen. Menetelmän johdosta algoritmin salaus on nopea ja turvallinen. Kyseistä algoritmia käytetään etäkäyttöohjelmissa liikenteen salaamiseen. (RSA Laboratories)

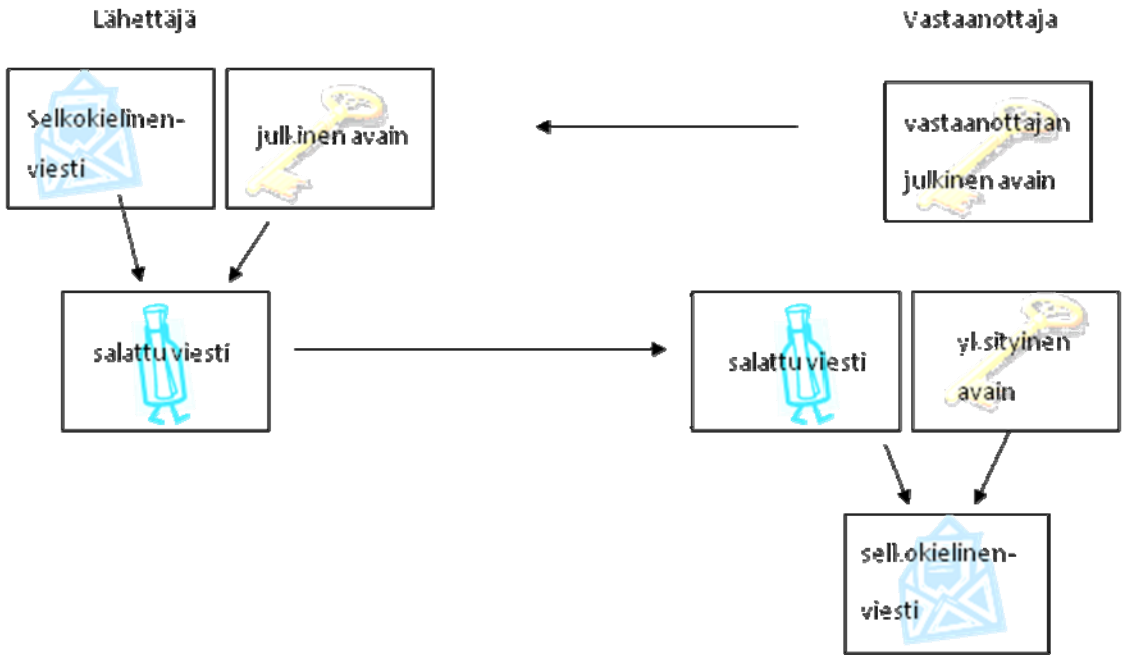
Aloite AES (Advanced Encryption Standard) algoritmista tehtiin vuonna 1997. NIST (National Institute of Stadards and Technology) järjestön tavoitteena oli saada AES algoritmista standardi, joka pysyisi turvallisena seuraavalle vuosisadalle. Vuonna 2001 valittiin AES-algoritmiksi, Joan Daemen ja Vincent Rijmen kehittämä Rijndael algoritmi. DES algoritmin tavoin AES on myös lohkosalausalgoritmi. AES tukee 128, 192 ja 256-bittisiä avainkokoja DES algoritmin 56-bitin avaimenlisäksi. Etäkäytössä AES salausta käytetään liikenteen salaamiseen. (RSA Laboratories)

4.2.2 Asymmetrinen salaus

Asymmetrisen eli epäsymmetrisen salauksen kehittivät Whitfield Diffie ja Martin Hellman v.1976. Salausmenetelmä mahdollistaa kahden osapuolen vaihtaa avaimia turvattoman verkon ylitse. Menetelmä on altis kolmannen osapuolen hyökkäykselle (man-in-the-middle). DH76 –salausmenetelmää käytetään muiden todennusmenetelmien kanssa suojaamaan IP-liikennettä. (RSA Laboratories)

Vuotta myöhemmin kehitettiin yksi suosituimmista epäsymmetrisen salauksen algoritmeista RSA. RSA nimi tulee tekijöiden sukunimien ensimmäisistä kirjaimista Ronald L. Rivest, Adi Shamir ja Leonard Adelman. Menetelmä perustuu suurten lukujen tekijöiden jakamisen vaikeuteen. (RSA Laboratories)

Asymmetrinen salaus käyttää kahta eri avainta (kuvio 6): salaista (private key) ja julkista (public key). Avaimet ovat vaihtokelpoisia siten, että julkisella avaimella salattu viesti voidaan avata kyseessä olevan avainparin yksityisellä avaimella ja päinvastoin. Salattaessa sähköpostiviestiä, viesti ensin salataan vastaanottajan julkisella avaimella, jonka jälkeen viesti voidaan lähettää vastaanottajalle. Vastaanottaja avaa viestin omalla salaisella avaimellaan. Koska salainen avain on ainoastaan vastaanottajan hallussa, ei kukaan ulkopuolinen pysty lukemaan salattua viestiä. (Viestintävirasto 2001)



KUVIO 6. Asymmetrisen salauksen toiminta

Asymmetrisen salauksen suurimpana heikkona puolena on menetelmän hitaus. Hyvänä puolena asymmetrisessä salauksessa on avaintenhallinnan yksinkertaisuus. Julkisen avaimen levittäminen on turvallista, koska salatun viestin aukaisu julkisella avaimella ei onnistu. Menetelmässä välttämätöntä on ainoastaan yksityisen avaimen säilyttäminen turvassa. (Viestintävirasto 2001)

4.2.3 Tiivistysalgoritmit

Tiivistysalgoritmit (hash function) tuottavat vaihtelevan mittaisesta tiedosta vakiomittaisen tiivisteen (RSA Laboratories). Algoritmia käytetään eheyden tarkistukseen, salasanojen talletukseen tai osana digitaalista allekirjoitusta. (Unixwiz.net - Software Consulting Centeral). Yleisimpiä käytettyjä tiivistysalgoritmeja ovat MD5, SHA, HMAC.

5 ETÄKÄYTTÖOHJELMAT

Vertailuun valittiin ilmaisia ja maksullisia etäkäyttöohjelmia, jotka toimivat lähiverkossa (Liite 3). Lähtökohtana oli, että lähiverkossa toimivat etäkäyttöohjelmat eivät tarvitse kolmatta osapuolta yhteyden muodostamiseen. Ilmaisella etäkäyttöohjelmalla puolestaan viitataan ohjelman hintaan. UltraVNC, TightVNC ja Etätyöpöytäyhteys olivat vertailun ilmaiset etäkäyttöohjelmat. Mukaan otettu RealVNC –ohjelma oli maksullinen. VNC –etäkäyttöohjelmien ja etätyöpöytäyhteyden lisäksi valitsimme vertailtavaksi TeamViewer ja NetOp –etäkäyttöohjelmat.

5.1 Etätyöpöytäyhteys

Etätyöpöytäyhteys on Microsoft Corporationin kehittämä etäkäyttöohjelma. Ohjelman testattu versio oli 6.0 ja se käyttää RDP kuljetuskerrosta. Yhteyden salaamiseen käytetään 56 tai 128-bittistä RC4 salausta. Etätyöpöytäyhteys palvelinohjelma löytyy sisällytettynä vain Windows XP Professional ja Vista käyttöjärjestelmistä. Asiakasohjelma on mahdollista ladata ilmaiseksi Windows 95 ja sitä uudempiin käyttöjärjestelmiin. Ongelmatilanteissa apua tarjoavat ohjelman suomenkieliset ohjeet, ohjelman valmistajan keskustelufoorumit ja tietämyskanta (knowledgebase) sekä puhelintuki.

5.2 NetOp Remote Control

NetOp Remote Control on Tanskalaisen Danware A/S kehittämä etäkäyttöohjelmisto. NetOp RC versio 9 käyttää DTL -protokollaa, joka on Danwaren itse kehittämä protokolla. Ohjelmisto koostuu useasta ohjelmasta, joista vertailtavaksi on valittu ainoastaan palvelin ja asiakasohjelma. Ohjelmistosta on saatavilla 30 päivän testiversio, mutta muuten se on maksullinen. NetOp RC -ohjelmistossa käytetään yhteyden salaamiseen 2048-bittistä Diffie-Hellman –avaimen vaihtoa, 256-bittistä AES -salausta ja SHA MAC -eheyden tarkistusta.

NetOp RC -ohjelmisto tukee Windows-pohjaisia käyttöjärjestelmiä ja rajoitetusti Linux-, Solaris- ja Symbian käyttöjärjestelmiä. Ohjelmiston ohjeet ja käyttöliittymä on saatavilla suomen- ja englanninkielellä. Tarjolla on myös suomenkielinen puhelin- ja sähköpostituki sekä englanninkielinen tietämyskanta.

5.3 RealVNC

RealVNC -etäkäyttöohjelmisto on RealVNC Limited nimisen yrityksen kehittämä VNC -pohjainen ohjelmisto. RealVNC käyttää VNC -protokolla 4.0 versiota, joka on jatkokehitetty RFB -protokollasta. RealVNC –etäkäyttöohjelman ilmaisversio on hyvin karsittu, sillä siitä puuttuu yhteyden salaus ja Vista tuki. Testikappale oli RealVNC Enterprise Edition 4.3.2 version, josta löytyi 2048-bittinen RSA tunnistus ja 128-bittinen AES liikenteen salaus sekä Vista tuki. Suomenkielisiä ohjeita tai käyttöliittymää ei ollut tarjolla, mutta maksullisessa versiossa voi nettisivujen kautta jättää tukipyynnön johon vastataan sähköpostilla. Tukipyynnöt täytyi jättää englanninkielellä.

5.4 TeamViewer

TeamViewer on TeamViewer GmbH kehittämä etäkäyttöohjelma. Testatussa versiossa 3.0793 on käytössä valmistajan oma protokolla eikä se ole yhteensopiva vanhempien versioiden kanssa, jotka pohjautuivat RFB -protokollaan. TeamViewer on ilmainen henkilökohtaiseen ja ei kaupalliseen käyttöön. Käyttäjän tunnistuksessa käytetään 1024-bittistä RSA salausmenetelmää ja yhteys on salattu 128-bittisellä RC4 -salausmenetelmällä. Ohjeita oli saatavilla englanniksi sekä saksaksi ja käyttöliittymä oli englanninkielinen. Ongelma tilanteissa valmistajan sivuilla voi jättää tukipyynnön tai soittaa palvelu- ja tukinumeroihin.

5.5 TightVNC

TightVNC on pienen ryhmän kehittämä RFB –pohjainen etäkäyttöohjelmisto. Testattu ohjelmisto versio 1.3.9 käyttää RFB 4.0tight protokollaa. Ohjelmisto toimii Windows, Unix ja Linux käyttöjärjestelmissä. Vista-tukea ei ole tällä hetkellä saatavilla. Käyttäjän tunnistus on mahdollista suorittaa ainoastaan VNC
-tunnistuksella, jossa salasanan pituus on rajoitettu kahdeksaan merkkiin. Yhteyden salausta ei ohjelmistossa ole. Ohjeistus ja käyttöliittymä ovat englanninkielisiä. Ongelma tilanteissa apua tarjoaa ohjelmiston kotisivuilta löytyvä englanninkielinen postituslista ja usein kysyttyjä kysymyksiä osio.

5.6 UltraVNC

UltraVNC on pienen ryhmän kehittämä VNC -pohjainen etäkäyttöohjelmisto. Ohjelmisto pohjautuu pääosin RealVNC –etäkäyttöohjelmiston 3.3.6 ja 3.3.7 versioihin. UltraVNC tukee Windows 9x/NT/ME/2000/XP käyttöjärjestelmiä. Windows Vista tukea ei löytynyt testatusta 1.02 versiosta, joka on viimeisin virallinen julkaistu versio. Vista tuki on kuitenkin tulossa beta-testeissä olevassa 1.04 versiossa.

Ohjelmassa käyttäjän tunnistus on mahdollista suorittaa VNC -tunnistuksella, käyttäen paikallisia tai toimialueen käyttäjätilejä. Yhteyden salaus onnistuu ainoastaan erillisillä lisäosilla, joista asennusohjeita ja tietoa löytyy virallisten sivujen kautta. UltraVNC –ohjelmiston käyttöliittymä ja ohjeet ovat englanninkielisiä. Valmistajan sivuilla on keskustelufoorumit, minne ongelmatilanteissa voi esittää kysymyksiä.

6 VERTAILUTAVAT

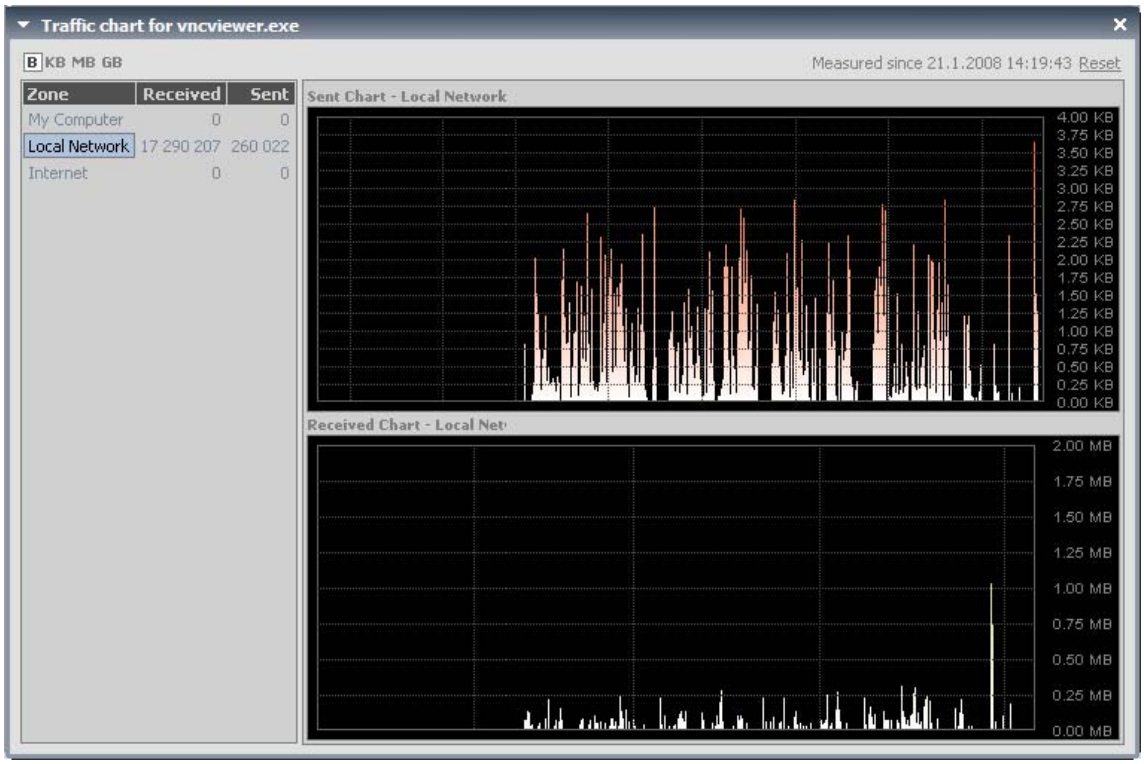
Ohjelmiin tutustumisen jälkeen, tapahtui ohjelmien välinen vertailu. Etäkäyttöohjelmistojen kesken vertailussa oli toteutettu asennettavuus, käytettävyys, tietoturva, verkon käyttö ja hinta.

Etäkäyttöohjelmistojen asennuksissa huomio kiinnittyi oletusasetusten riittävyyteen asennuksessa. Lisäksi tarkasteltavia asioita olivat asennusohjelmien asennuskieli ja ongelmatilanteet.

Käytettävyyttä arvioitiin ohjelman ominaisuuksien, helppokäyttöisyyden, käyttäjätuen ja etäyhteyden toimivuuden kautta. Käytettävyys testattiin ohjelmien oletusasetuksilla. Ohjelmista tuli olla erillinen palvelin- ja asiakasohjelma ohut asiakas -mallin mukaisesti. Käyttäjätukea tarkasteltaessa tutkittiin ohjelman käyttöohjeiden kattavuutta ja ongelmatilanteita varten olevia palveluita. Etäyhteyden toimivuutta tutkittiin, kiinnittämällä huomiota yhteyden yleiseen toimivuuteen, kuvan päivittymiseen ja mahdollisiin virhe- sekä ongelmatilanteisiin.

Tietoturva kohdassa tarkasteltiin salausten toimintaa käyttäen Wireshark ohjelmaa. Wireshark -ohjelman avulla pystyttiin seuraamaan etäkäyttöohjelman keskustelua asiakkaan ja palvelimen välillä (Liitteet 1 ja 2). Salausta ei ollut käytössä, mikäli viestit ovat selkokielisiä. Itse salaukset ja niiden vahvuudet selvitettiin ohjelmistojen tekijöiden ja jakelijoiden sivujen kautta. Tässä osiossa tutkittiin myös, kuinka ohjelmat ovat hoitaneet käyttäjän tunnistuksen.

Verkon käyttöä mitattiin Netlimiter 2 –ohjelmalla etäkäyttöyhteyden avauduttua. Mittaus hetkellä etäkäyttöohjelman käyttö tapahtui oletusasetuksilla. Mittaus suoritettiin seuraavalla tavalla: MS Office 2007 käyttö, PPPoE -asiakasohjelman avaaminen, selaimen käyttö, kirjautuminen ulos ja kirjautuminen sisään. Jokaisen ohjelman mittauksen jälkeen odotettiin n. 5 s ennen kuin siirryttiin testauksessa eteenpäin. MS Office –ohjelmistosta käytiin läpi seuraavat ohjelmat seuraavanlaisessa järjestyksessä Word, Excel, PowerPoint. Office –ohjelmalla avattiin valmiiksi kirjoitettu tai kuvitettu tiedosto. Avattuun tiedostoon muokattiin sivuasetuksia, kirjoitettiin tekstiä ja suljettiin ohjelma. Mittaus selaimen käytöstä tehtiin Internet Explorer 6 –selaimella. Selaimella siirryttiin osoitteeseen http://www.kopioniini.fi/. Sivun avauduttua suljettiin selain ja kirjauduttiin ulos Windows käyttäjätililtä. Windows sisäänkirjautumisruudun tullessa näkyviin, kirjauduttiin takaisin sisään. Kuviossa 7 on Netlimiter 2-ohjelman tuloste verkonkäytöstä. Tulosteen perusteella laadittiin verkonkäytön vertailu etäkäyttöohjelmien välillä.



KUVIO 7. Netlimiter -diagrammi verkonkäytöstä

Lopuksi vertailtiin etäkäyttöohjelmistojen maksullisuutta. Mikäli ohjelman käyttö oli maksullista, selvitettiin ohjelman hinta ottaen huomioon toimeksiantajan tarpeet.

7 ETÄKÄYTTÖOHJELMIEN VERTAILU

Ennen etäkäyttöohjelmien vertailua luotiin etäkäyttöympäristö ohjelmille. Käyttöympäristön luomiseksi tarvittiin asiakas- ja palvelinohjelmalle erilliset käyttöjärjestelmät. Etäkäyttöympäristö luotiin yhdelle tietokoneelle, johon oli asennettu Windows XP Professional -käyttöjärjestelmä. Tämä käyttöjärjestelmä toimi etäkäyttöympäristössä asiakaskoneena. Asennettiin Windows XP Professional ja Windows 2000 -käyttöjärjestelmät virtuaalisesti käyttäen Microsoft Virtual PC ohjelmaa. Kyseinen virtuaalisesti asennettu Windows XP Professional käyttöjärjestelmä toimi etäkäyttöympäristössä palvelimena. Windows 2000 – käyttöjärjestelmää käytettiin selvittämään ohjelmien toimivuus kyseisessä käyttöjärjestelmässä.

Käyttöjärjestelmäasennusten jälkeen asetettiin palvelin- ja asiakaskäyttöjärjestelmät samaan verkkoon sekä asennettiin palvelimelle F-Secure Client Security tietoturvaohjelmisto ja MS Office 2007 Professional ohjelmisto. Tietoturvaohjelmiston suojaustasona käytettiin ohjelman oletustasoa.

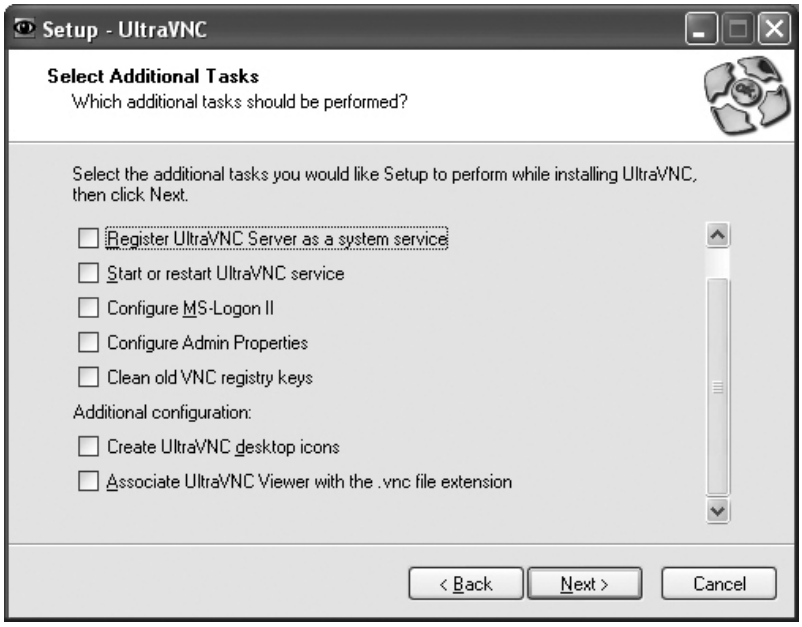
7.1 Asennettavuus

Ohjelmiston asennus on ensimmäinen vaihe mihin törmätään, kun on hankittu etäkäyttöohjelmisto. Asennusohjelma on ensimmäinen asia, mikä erottaa ohjelmat toisistaan. Selvimmät erot etäkäyttöohjelmien välillä näkyivät asennusohjelman helppokäyttöisyydessä ja asennusohjelman kielen valinnoissa. Taulukossa 1 on esitelty etäkäyttöohjelmien asennettavuuden arvosanat.

TAULUKKO 1. Etäkäyttöohjelmien asennettavuuden arvosanat.

Ohjelma	Arvosana
RealVNC	4
TeamViewer	4
NetOp	3
TightVNC	2
UltraVNC	2
Etätyöpöytäyhteys	1

UltraVNC ja TightVNC –ohjelmistoissa asennusohjelmat olivat hyvin yhtenevät, ja täten kyseisten ohjelmistojen asennus on arvioitu yhdessä. UltraVNC ja TightVNC ohjelmistojen asennus sisälsi paljon vaiheita, toimintoja ja valintoja. Asennusohjelman kielenä oli englanti, mikä hidasti asennusta oleellisesti. Osa valinnoista oli tehtävä asennuksen yhteydessä, sillä asennuksen jälkeen tehtyjä valintoja ei päässyt enää vaihtamaan. Kuviossa 8 on kuvattu UltraVNC etäkäyttöohjelmiston asennusohjelman yhden vaiheen eri vaihtoehtoja. UltraVNC ja TightVNC molemmat saivat asennettavuuden arvosanaksi 2.



KUVIO 8. UltraVNC -ohjelmiston asennuksen vaihtoehtoja

NetOp RC –etäkäyttöohjelmiston asennus oli suomenkielinen, mutta paikoin hyvin epäselvä ja sekoittava. NetOp -ohjelmiston asennus tapahtui kahdessa vaiheessa. Ensimmäisessä vaiheessa täytyi valita asennettavat NetOp –ohjelmiston ohjelmat. Toisessa vaiheessa asennettiin yksitellen jokainen valittu ohjelma. Asennusohjelmassa olisi pitänyt olla paremmin esillä asiakas ja palvelinohjelman asennus. Useat vaihtoehdot ohjelmien välillä sekoittivat turhaan asennusta. Tästä NetOp ohjelmistolle arvosanaksi 3.

Vertailun ainoa etäkäyttöohjelma jonka palvelinohjelmaa ei ollut mahdollista asentaa, oli etätyöpöytäyhteys. Etätyöpöytäyhteys ohjelmasta oli kuitenkin mahdollista asentaa asiakasohjelma. Etätyöpöytäyhteys ansaitsee tästä asennettavuuden arvosanaksi 1.

Vertailun helpoimmat asennettavat etäkäyttöohjelmistot olivat TeamViewer ja RealVNC. Molemmissa ohjelmistoissa asennus oli mahdollista suorittaa hyvin vähällä tiedon syöttämisellä. Asennusohjelmien kieli oli englanti. RealVNC ohjelmiston asennusta hankaloitti asennusvalintojen selitysten puuttuminen. Molemmat ohjelmistot saivat asennuksen arvosanaksi 4.

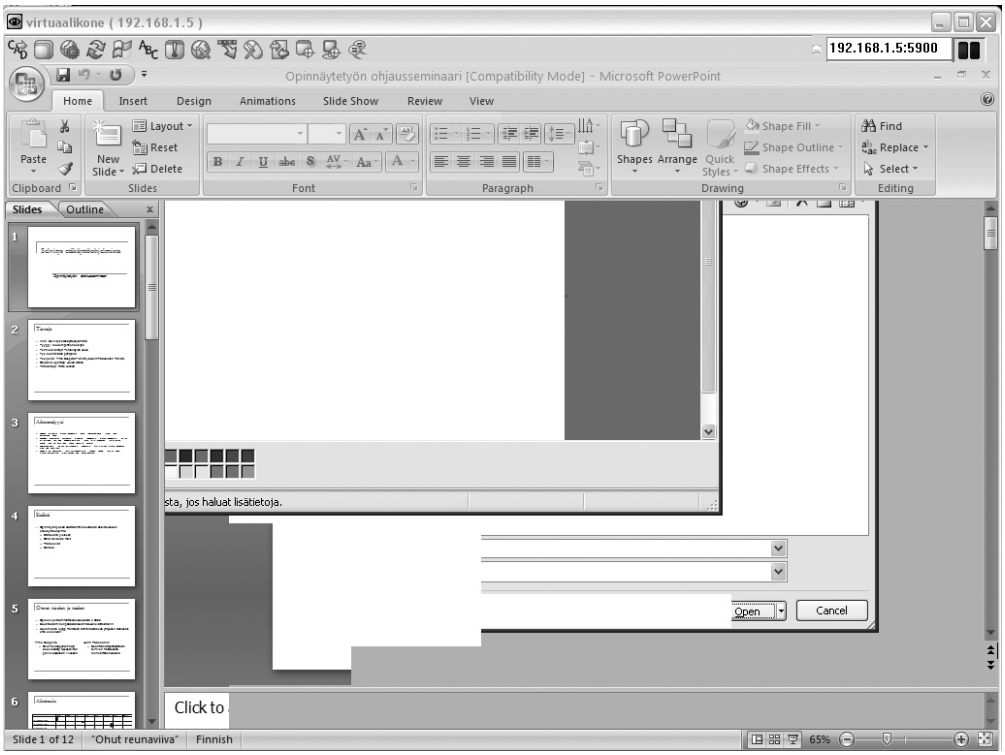
7.2 Käytettävyys

Käytettävyyden vertailussa maksulliset ohjelmat olivat helppokäyttöisempiä kuin ilmaiset ohjelmat. Ohjelmien asetukset, toimivuus, dokumentaatio ja tukipalvelut erottivat ohjelmat toisistaan. Taulukossa 2 on nähtävillä ohjelmien käytettävyyden arvosanat.

TAULUKKO 2. Etäkäyttöohjelmien käytettävyyden numerot.

Ohjelma	Arvosana
NetOp	5
RealVNC	4
TeamViewer	3
TightVNC	2
UltraVNC	2
Etätyöpöytäyhteys	1

UltraVNC –ohjelmiston asetukset olivat mielestämme erittäin huonosti esillä. Ohjelman dokumentaatio ja ohjeet olivat puutteelliset ja vaikeasti saatavilla. Tämä vaikeutti entisestään ohjelman käyttämistä. UltraVNC –ohjelmistoa käyttäessä, PowerPoint ei kyennyt päivittämään dian esitysaluetta (kuvio 9). Valmistajan kotisivuilta löytyvä keskustelupalsta tuli erittäin tutuksi. Sieltä löytyi vastaus lähes kaikkiin ohjelman käytöstä heränneisiin ongelmiin. Käytettävyydestä UltraVNC sai arvosanaksi 2.



Kuvio 9. UltraVNC –ohjelmiston piirtovirheet PowerPoint –ohjelmassa.

TightVNC -ohjelmassa oli vastaavanlaisia kuvanpiirto-ongelmia, kuin UltraVNC –ohjelmassa. Ongelmat ilmenivät Office 2007 ja internet selaimen käytössä. Ohjelma ei kyennyt näyttämään missään testattavassa Office 2007 ohjelmassa alaspudotusvalikkoa. Tämä tekee Officen käytön lähes mahdottomaksi. Tämän lisäksi TightVNC kykeni päivittämään vain ensimmäisen näkymän selaimen avaamasta sivusta, joka piti sisällään kuvia. Sivua kun vieritettiin ylös tai alaspäin, sivuilla olevat kuvat suttasivat näkymän. Etäyhteyttä ei ollut mahdollista muodostaa, mikäli palvelinkone oli Windows-kirjautumisruudussa ja käytössä oli manuaalinen yhteyden varmentaminen. Itse ohjelman käytössä asetukset olivat luokiteltu hyvin välilehtien alle, mikä helpotti ohjelman käyttämistä. Lisäksi tuen puuttuminen ja puutteellinen dokumentaatio vähensi käytettävyyttä. TightVNC sai arvosanaksi 2.

TeamViewer –etäkäyttöohjelmisto oli vertailun hankalin ohjelma ottaa käyttöön. Käyttöönotto vaati avoimena olevan internetyhteyden. Ohjelmisto koostui yhdistetystä asiakas ja palvelin ohjelmasta. Ohjelmiston asetukset koostuivat vain sille tärkeimmistä asetuksista, ja ne oli jaoteltu selkeästi välilehtien alle. Ohjelmiston ohjeet olivat vain englanninkielellä ja löytyivät vain verkosta. Tämä hankaloitti hieman sen käyttämistä. Ohjelmaa käytettäessä ei havaittu ongelmatilanteita. Arvosanaksi TeamViewer sai 3.

RealVNC oli käytettävyydeltään VNC –ohjelmien parhaimmistoa. Asiakas- ja palvelinohjelman asetukset olivat helposti löydettävissä ja luokiteltu välilehtiin. Poikkeuksena muihin VNC

ohjelmiin, asiakasohjelmassa oli mahdollista tallentaa asetukset erilliseen tiedostoon. Asiakasohjelmalla pystyi myös lataamaan talletettuja asetuksia. Ohjelman dokumentaatio tuli asennuksen yhteydessä ja oli helposti löydettävissä. Dokumentaatio oli mielestäni erittäin hyödyllinen ja käytännöllinen. Etäkäyttöyhteyden avattua ruudun päivitys oli sulavaa emmekä havainneet ongelmia muodostuneessa yhteydessä. RealVNC arvosanaksi 4.

Etätyöpöytäyhteys ohjelma oli NetOp –etäkäyttöohjelman rinnalla vertailun ainoat suomenkieliset etäkäyttöohjelmat. Windows 2000 – käyttöjärjestelmän etäkäyttö ei ollut mahdollista etätyöpöytäyhteydellä, koska käyttöjärjestelmä ei sisältänyt etätyöpöytäyhteyden palvelinohjelmaa. Etätyöpöytäyhteys asiakasohjelman asetukset olivat hyvin esillä. Palvelinasetusten löytäminen ja säätäminen vaativat hieman aikaa. Ohjelman ohjeet olivat suomenkieliset ja helposti löydettävissä. Ohjelma lukitsee palvelintyöaseman, kun etäkäyttöyhteys muodostetaan onnistuneesti. Etätyöpöytäyhteys ei myöskään kysy käyttäjältä lupaa työasemalle kirjautumiseen, eikä anna ilmoitusta päättyneestä etäkäyttötilanteesta. Tämä vähensi ohjelman käyttömahdollisuuksia oleellisesti. Vaikka, etäkäytössä ei havaittu ongelmatilanteita, etätyöpöytäyhteys sai käytettävyyden arvosanaksi 1.

Suomenkielinen NetOp Remote Control piti sisällään paljon hyödyllisiä toimintoja ja asetuksia liittyen etäkäyttöön ja etenkin tukitoimintaan. NetOp -ohjelmistoa voi kuvailla tukihenkilön työkaluksi. Asiakasohjelmalla oli mm. mahdollista luoda ja hallita yhteystietoja, ottaa vastaan tukipyyntöjä, nauhoittaa ja katsoa menneitä etäkäyttötapahtumia. NetOp asiakasohjelmassa yhteyden muodostus palvelimeen oli rakennettu mahdollisimman yksinkertaiseksi. Siinä oli mahdollista selata NetOp tai Windows-verkkoa, ja näin yhdistää haluamaansa NetOp -palvelimeen. Palvelinohjelmalla puolestaan oli mahdollista lähettää etätuki-pyyntö samassa verkossa sijaitseville NetOp asiakasohjelmille. Lähetetystä tukipyynnöstä tuli ilmoitus asiakasohjelmaan, jossa se voitiin käsitellä. NetOp –ohjelman ohjeet olivat englanninkieliset ja mielestämme vertailun parhaimmistoa. NetOp –ohjelman kuvan päivitys oli sulavaa ja käytössä emme havainneet ongelmatilanteita. Käytettävyydestä NetOp RC –ohjelmisto sai arvosanaksi 5.

7.3 Tietoturva

Tietojen turvaaminen on tärkeää ja etäkäyttö onkin hyvin tärkeä suojata, ettei asiattomat pääsisi käsiksi tietoihin, jotka voisivat olla vahingollisia joutuessa vääriin käsiin. Taulukossa 3 on nähtävillä tietoturvan arvosanat.

TAULUKKO 3. Etäkäyttöohjelmien tietoturvan arvosanat.

Ohjelma	Arvosana
NetOp	5
RealVNC	4
TeamViewer	3
UltraVNC	3
Etätyöpöytäyhteys	2
TightVNC	1

Kaikissa ohjelmissa käyttäjän tunnistus oli tehty niin, ettei salasanoja välitetty selkokielisenä verkon yli. Käyttäjän tunnistuksessa oli huomattaviakin eroja ohjelmien kesken. UltraVNC ja TightVNC –ohjelmistoissa käytetyssä VNC-tunnistuksessa salasanan pituus oli rajattu kahdeksaan merkkiin. Mikäli UltraVNC –ohjelmistossa oli käytössä jokin salaus, salasanan tuli olla tasan kahdeksan merkkiä pitkä. Testatussa RealVNC –ohjelmistossa tätä ongelmaa ei ollut, vaan salasana pystyi olemaan 255 merkkiä pitkä. Käyttäjän tunnistuksessa UltraVNC ja RealVNC mahdollistivat paikallisen käyttäjätilin tai toimialueen käyttäjätilin käyttöä. Toteutus käyttäjätilin ja toimialueen käytössä erosi dokumenttien mukaan, mutta käytännössä kyseistä ominaisuutta ei testattu. Paikallisen käyttäjätilin tietoja käyttäjän tunnistuksessa käytti myös etätyöpöytäyhteys.

TeamViewer –ohjelman käyttäjän tunnistus tapahtui oletusasetuksilla hivenen muista poikkeavalla tavalla. Ohjelman käynnistyessä, se loi automaattisesti salasanana toimivan istuntoavaimen joka vaihtui ohjelman uudelleenkäynnistykseen jälkeen. Tämän pystyi korvaamaan kiinteällä salasanalla, jota käytettiin istunnoissa käyttäjän tunnistamiseen.

NetOp Remote Control -ohjelmistossa oli mahdollista luoda käyttäjätunnukset ja salasanat sekä rajoittaa käyttäjien oikeuksia paikallisesti. Käyttäjätietoja pystyttiin myös ylläpitämään erillisellä palvelimella keskitetysti, mutta tätä ominaisuutta ei testattu. Käyttäjätietojen keskitys olisi vaatinut erillisen ohjelman. Käyttäjän tunnistus koostui kuudesta mahdollisesta vaiheesta: MAC/IP-osoitteen tarkastaminen, ohjelmiston sarjanumeron tarkastaminen, käyttäjän tunnistaminen, varmennussoitto yhteydenottajalle, yhteyden manuaalinen varmentaminen ja käyttäjän valtuuksien tarkastaminen. Kaikki ohjelmat paitsi TeamViewer ja etätyöpöytäyhteys sisälsivät yhteyden manuaalisen varmentamisen. Etäyhteyden muodostuessa palvelimelle tuli kysely yhteyden hyväksymisestä tai hylkäämisestä.

Yhteyden salausta ei kaikissa ohjelmissa ollut. UltraVNC ja TightVNC eivät oletusarvoisesti sisältäneet minkäänlaista yhteyden salausmahdollisuutta, mikä on turvattoman verkon yli tietoturvariski. UltraVNC –ohjelmistoon oli saatavilla lisäosana ilmaisia yhteyden salausmahdollisuuksia. RealVNC, TeamViewer, NetOp ja Etätyöpöytäyhteys pitivät sisällään

yhteyden salauksen eikä niiden päälle asettaminen vaatinut asetusten muuttamista. Salaustavoissa ja niiden vahvuuksissa oli huomattavia eroja. NetOp –ohjelmisto käytti istunnon salaamiseen 256 -bittistä AES-algoritmia, siirrettävä tieto ajettiin 160 tai 256 –bittisen SHA HMAC integraatiotarkastuksen läpi ja tiedon salaamiseen käytettiin 2048 –bittistä Diffie-Hellman avaimenvaihtoa. TeamViewer käytti 1024 –bittistä RSA avaimenvaihtotekniikkaa tiedonsalaukseen ja 128 –bittistä RC4 salausta istuntojen salaamiseen. RealVNC käytti 128 –bittistä AES -algoritmia yhteyden salaamiseen ja 2048 –bittistä RSA avaimenvaihtoa palvelimen varmentamiseen.

Etätyöpöytäyhteyden istunnot oli salattu 56 tai 128 –bittisellä RC4 salauksella. UltraVNC –ohjelmistoon lisäosana saatavia salauksia oli 40, 56 tai 128 –bittinen RC4 ja 128 –bittinen AES salaus. Molemmilla menetelmillä oli myös mahdollista itse luoda salausavain. Jotta yhteys voitiin muodostaa, avain tuli jakaa palvelin- ja asiakaskoneille. Avaimen jakaminen tuli suorittaa manuaalisesti.

Tietoturvan parhaimmistoa edusti NetOp RC. Siinä käytetyt salaukset ja käyttäjän tunnistus olivat vahvoja. Lisäksi NetOp RC sisälsi ainoana ohjelmistona tiedon eheyden tarkistuksen. Näillä perusteilla NetOp -ohjelmistolle arvosana 5. Myös TeamViewer ja RealVNC sisälsivät vahvoja salausmenetelmiä ja käyttäjän tunnistuksen, joka oli turvallisesti hoidettu. RealVNC sisälsi myös käyttäjän manuaalisen varmentamisen, mikä oikeutti sille arvosanan 4. TeamViewer ei sisältänyt manuaalisen varmennuksen mahdollisuutta ja sen koettiin olevan heikkous. Teamviewer sai arvosanan 3. Etätyöpöytäyhteydessä käytettiin tiedonsiirtoon jonosalausta ja arvosanaksi se sai 2. UltraVNC käytti lisäosissa vähintään yhtä vahvaa salausta kuin etätyöpöytäyhteys, mutta lisäominaisuutena ollut avain loi lisää tietoturvaa. Kuitenkin lisäosien toimintaan asettaminen vaati aikaa ja tutustumista ohjeisiin. Salauksen asettaminen suuremmille määrille koneita ilman automaattisesti asentuvaa pakettia kuluttaa hyvin paljon aikaa. Tämän takia se sai arvosanaksi 3. TightVNC oli ainoa, jossa yhteyttä ei ollut mahdollista salata. Tämän vuoksi se sai arvosanaksi 1.

7.4 Verkonkäyttö

Verkon siirtokapasiteetin tiputtua, useat etäkäyttöohjelmat kykenevät mukautumaan verkon nykyiseen siirtokapasiteettiin. Tämä kuitenkin tapahtui kuvalaadun heikentämisenä ja tiedon pakkauksen lisääntymisellä. Ohjelman mukautuessa verkon nykyiseen siirtokapasiteettiin, se voi vaurioittaa käynnissä olevaa etätapahtumaa ja katkaista yhteyden. Taulukossa 4 on nähtävillä etäkäyttöohjelmien verkonkäytön arvosanat.

TAULUKKO 4. Etäkäyttöohjelmien verkonkäytön arvosanat.

Ohjelma	Arvosana
TeamViewer	5
TightVNC	4
Etätyöpöytäyhteys	3
NetOp	2
RealVNC	2
UltraVNC	1

TeamViewer ja Etätyöpöytäyhteys edusti vertailun parhaimmistoa verkonkäytön osalta. Oletusasetuksilla molemmat ohjelmistot vastaanotti tietoa keskimäärin vain 27 kB/s. UltraVNC puolestaan oli vertailun huonoin ja käytti verkkoa keskimääräisesti eniten. UltraVNC lähetti dataa 1 kB/s ja vastaanotti 250 kB/s. Taulukossa 5 on kuvattu etäkäyttöohjelmien verkonkäyttö. Siitä voi havaita, kuinka vähäistä on etäkäyttöohjelmien tiedon lähetys suhteessa tiedon vastaanottoon. Vertailtujen ohjelmien välillä ei ollut suuria eroja tiedon lähetyksessä.

TAULUKKO 5. Etäkäyttöohjelmien verkonkäyttö keskimäärin (kB/s).

Ohjelma	Lähetys	Vastaanotto
TeamViewer	1	27
Etätyöpöytä	2	27
TightVNC	1	35
RealVNC	1,5	125
NetOp	2,3	125
UltraVNC	1	250

Taulukon 6 mukaan, etäkäyttöohjelmien väliset erot kasvoivat hieman, kun mitattiin verkonkäyttöä maksimissaan. Testissä TightVNC pärjäsi muita etäkäyttöohjelmia paremmin ja vastaanotti hetkellisesti 95 kB/s. TeamViewer sijoittui toiseksi vastaanottamalla tietoa hetkellisesti 135 kB/s. Etätyöpöytäyhteys oli testin yllättäjä ja siirsi hetkellisesti tietoa asiakkaalta palvelimelle 23 kb/s ja palvelimelta asiakkaalle 397 kb/s. NetOp ja RealVNC molemmat sijoittuivat myös maksimaalisessa verkonkäytössä samoille sijoille lähettäen 3,75 kB/s ja vastaanottaen 1 000 kB/s. UltraVNC oli maksimaalisessa verkonkäytön testauksessa vertailun raskain.

TAULUKKO 6. Etäkäyttöohjelmien verkonkäyttö maksimissaan (kB/s).

Ohjelma	Lähetys	Vastaanotto
TightVNC	2,75	95
TeamViewer	1,75	135
Etätyöpöytä	23	397
NetOp	3,75	1 000
RealVNC	3,75	1 000
UltraVNC	2,5	1 250

Verkonkäytön vertailussa parhaiten pärjäsi TeamViewer, joka käytti verkkoa keskimääräisesti ja hetkellisesti vähiten. Tästä se sai arvosanaksi 5. Vertailussa toiseksi sijoittui TightVNC. Sen vakaa ja vähäinen verkonkäyttö oikeutti arvosanan 4. Etätyöpöytäyhteys ohjelman keskimääräinen verkonkäyttö oli vertailun vähäisintä. Ohjelma kuitenkin yllätti verkonkäytön maksimaalisessa käytössä ja näin sai arvosanaksi 3. Vertailun tasainen parivaljakko oli RealVNC ja NetOp. Molemmat ohjelmistot saivat arvosanaksi 2. UltraVNC oli vertailun raskain ohjelma ja sai arvosanaksi 1.

7.5 Hinta

Vertailussa olleiden etäkäyttöohjelmien hinnat vaihtelivat suuresti. Hinta-arviot suoritettiin maksullisissa versioissa neljälle tukihenkilökoneelle ja sadalle asiakaskoneelle. Taulukossa 7 on nähtävillä etäkäyttöohjelmien hinnan arvosana.

TAULUKKO 7. Etäkäyttöohjelmien hinnan arvosanat.

Ohjelma	Arvosana
UltraVNC	5
TightVNC	5
Etätyöpöytäyhteys	5
TeamViewer	4
RealVNC	3
NetOp	1

UltraVNC, TightVNC ja etätyöpöytäyhteys olivat ilmaisia, RealVNC -ohjelmistosta löytyy ilmainen versio, mutta se oli hyvin karsittu versio verrattuna testattuun RealVNC Enterprise

Editioniin. TeamViewer -ohjelmisto oli ilmainen yksityisessä ja ei kaupallisessa käytössä, mutta kaupalliseen käyttöön lisenssit oli hankittava. NetOp Remote Control -ohjelmistosta oli tarjolla 30 päivän esittelyversio, mutta muuten se oli täysin maksullinen ohjelma. Maksullisten ohjelmien lisensointimaksutkin erosivat hyvin suuresti. TeamViewer -ohjelmistoon ainoastaan tukihenkilö eli asiakas-ohjelma tarvitsi lisenssin. RealVNC -ohjelmiston lisensoinnissa maksettiin tuettujen koneiden eli palvelimien lisenssistä ja NetOp RC -ohjelmiston lisensoinnissa piti hankkia lisenssit sekä asiakas- että palvelinohjelmalle. Kirjoittamishetkellä NetOp RC -ohjelmiston lisenssien hinta oli yhteensä 4930 €. RealVNC -ohjelmiston lisenssien hinnaksi muodostui 1201.61 €, sivuilla olevan verkkolaskurin mukaan. TeamViewer lisenssien hinnaksi muodostui 796 €.

8 YHTEENVETO

Ilmaisten ja maksullisten etäkäyttöohjelmien väliset erot olivat vertailussa yllättävän suuria. Ilmaiset etäkäyttöohjelmat keskittyivät lähinnä etäyhteyden muodostamisen ja tarjosivat rajatusti etäkäyttöön liittyviä ominaisuuksia. Lisäksi ilmaisten ohjelmien heikkoutena oli vaikea käytettävyys ja alkeellinen salaus tai sen puuttuminen. Maksulliset ohjelmat puolestaan olivat helppokäyttöisempiä ja sisälsivät paremman tietoturvan. Suuria eroja oli myös ilmaisten ja maksullisten ohjelmien käyttäjätuessa. Ilmaisten ohjelmien tuen tarjoaminen tapahtui omilla keskustelupalstoilla tai pieninä tietämyskantoina. Maksulliset ohjelmat tarjosivat näiden lisäksi puhelin- ja sähköpostitukea. Etäkäyttöohjelmat on vertailtu painotetun keskiarvon mukaan. Painokertoimet verratuille kohteille saatiin toimeksiantajalta, he painottivat erityisesti tietoturvaa ja käytettävyyttä, koska nykypäivän yritysmaailmassa kaiken on oltava turvallista ja helppokäyttöistä. Arvoasteikolla 1 – 5, missä 1 oli huono ja 5 erittäin hyvä. Vertailun painokertoimet ja ohjelmien saamat arvosanat sekä painoarvot löytyvät taulukosta 8.

TAULUKKO 8. Vertailtujen etäkäyttöohjelmien painokertoimet, arvosanat ja painoarvo.

	Paino-kerroin	Etätyöpöytä-yhteys	NetOp	RealVNC	Team-Viewer	TightVNC	UltraVNC
Asennettavuus	2	1	3	4	4	2	2
Hinta	3	5	1	3	4	5	5
Käytettävyys	4	1	5	4	3	2	2
Tietoturva	5	2	5	4	3	1	3
Verkonkäyttö	1	3	2	2	5	4	1
Painoarvo		2,3	3,7	3,7	3,5	2,4	2,9

Painotetun keskiarvon perusteella voi sanoa, että NetOp RC ja RealVNC –ohjelmistot olivat vertailun parhaat etäkäyttöohjelmat. NetOp -ohjelmisto oli vertailun ylivoimaisesti hintavin, mutta samalla sisälsi ylivoimaisesti eniten ominaisuuksia ja vertailun parhaimman tietoturvan. Ominaisuuksien ja hinnan puolesta NetOp RC –ohjelmisto on hyvä etäkäyttöohjelma atk-tuelle yrityskäyttöön.

RealVNC –ohjelma oli VNC –ohjelmien parhaimmistoa. Vaikka ohjelman etuna oli vahva tietoturva ja käytettävyys sekä erillinen asiakas ja palvelin ohjelmisto. Se ei kuitenkaan pärjännyt käytettävyyden ja tietoturvan osalta NetOp –ohjelmistolle.

Vertailussa kolmanneksi sijoittui TeamViewer –ohjelma. Ohjelman etuna oli asennettavuus ja vähäinen verkon käyttö. TeamViewer –ohjelman käyttömahdollisuuksia rajoittaa kuitenkin se, että ohjelmassa on yhdistetty palvelin ja asiakasohjelma. Suuremmissa yrityksissä tämä voi muodostaa tietoturvariskin, koska jokainen tietokone voi toimia yhtäaikaisesti asiakkaana ja palvelimena. Vertailun tuloksena TeamViewer –ohjelma soveltuu parhaiten koti- tai pienyrityskäyttöön.

Ilmaisista etäkäyttöohjelmista parhaiten pärjäsi UltraVNC. UltraVNC –ohjelman etuna oli liitännäisten avulla saatava kohtalainen tietoturva ja erillinen asiakas- ja palvelinohjelma. Ohjelman käytettävyyttä kuitenkin rajoittaa hankala käytettävyys ja puutteellinen dokumentaatio. Puutteellisen dokumentaation takia ohjelman käytön opettelu vaati muita etäkäyttöohjelmia enemmän aikaa. Vertailun perusteella UtraVNC –ohjelmaa sopii hyvin yritys- ja yksityiskäyttöön.

TightVNC –ohjelman etuna oli vähäinen verkon käyttö. Salauksen puuttuminen teki ohjelman käytön turvattoman verkon yli vaaralliseksi. Salauksen puuttumisella on hyvin suora vaikutus ohjelman käytettävyyteen ja käyttömahdollisuuksiin. Lisäksi testeissä ohjelmalla oli vakavia kuvanpiirtoongelmia. Tämä rajoittaa ohjelman soveltuvuutta etäkäyttöön. Vertailun perusteella TightVNC –ohjelma soveltuu parhaiten käytettäväksi ohut asiakas -laitteilla suljetuissa verkoissa.

Heikoiten vertailussa pärjäsi Etätyöpöytäyhteys. Ohjelman etuna oli asiakasohjelman helppokäyttöisyys ja kohtalaisen tietoturvan löytyminen. Etätyöpöytäyhteys –ohjelman soveltuvuus atk-tuen käyttöön on kuitenkin kyseenalaista, sillä palvelimella oleva asiakas ei näe etäkäyttötapahtumaa. Asiakas ei myöskään saa minkäänlaista ilmoitusta muodostuvasta tai loppuneesta etäyhteydestä. Vertailun perusteella etätyöpöytäyhteys soveltuu parhaiten tilanteisiin, joissa palvelinkone ei ole aktiivisessa käytössä.

9 POHDINTA

Opinnäytetyön tarkoituksena oli tehdä selvitys etäkäyttöohjelmista Yritys X:lle. Otimme vertailtavaksi etäkäyttöohjelmia toimeksiantajan esittämien toiveiden mukaisesti. Työssä käsittelemme etäkäyttöohjelmia teknisestä ja ohjelmallisesta näkökulmasta. Vertailun tuloksena syntyi hankintaehdotus toimeksiantajalle.

Opinnäytetyön tekeminen aloitettiin jo alkukesästä 2007. Työskentely aloitettiin keräämällä materiaalia viitekehykseen ja luomalla käyttöympäristö etäkäyttöohjelmille. Kesäaika ja töiden tekeminen kuitenkin verotti motivaatiota tehdä opinnäytetyötä. Työn etenemistä hidasti myös viitekehyksen materiaalin saatavuuden vaikeus.

Loppusyksystä saimme alustavasti valmiiksi opinnäytetyön viitekehyksen. Työparini päätti lopettaa koulun kesken testausten jälkeen ja jäin yksin työn kanssa tämän takia. Vaikka materiaali oli pääosin kerätty ja opinnäytetyö oli periaatteessa kirjoittamista vailla oli työn loppuun saattaminen itsenäisesti erittäin suuri haaste.

Testausten aikana pidimme testauspäiväkirjaa, mikä osoittautui erittäin hyödylliseksi raportin kirjoitusvaiheessa. Ohjelmien testausta kuitenkin vaikeutti se, ettei kaikkia ohjelmia pystynyt pitämään yhtäaikaisesti asennettuina. Varsinkin VNC –pohjaiset etäkäyttöohjelmat jouduttiin testaamaan yksitellen ja poistamaan testauksen jälkeen.

Henkilökohtaisena tavoitteena opinnäytetyöllä oli oppia etäkäyttöohjelmien toimintaperiaatteet ja saada vertailukohtia etäkäyttöohjelmien soveltuvuudesta eri tilanteisiin. Tulosten mittaamiseen ja analysointiin käytimme työn aikana meille osittain ennalta tuntemattomia ohjelmia. Ohjelmien käytön opettelu vei ylimääräistä aikaa. Kyseisistä ohjelmista oli kuitenkin hyvin paljon apua, kun tarkastelimme etäkäyttöohjelmien liikennettä. Mielestäni henkilökohtaiset tavoitteet opinnäytetyölle täyttyivät hyvin.

Mielestäni opinnäytetyön tekeminen aiheesta onnistui, vaikka materiaalin saatavuus, ajan ja motivaation puute siirsivät aikatauluja. Maksullisten etäkäyttöohjelmien käyttämistä protokollista oli erittäin vaikea löytää materiaalia. Materiaalin hankinta oli mahdollista vain jos protokollan kehittänyt yritys luovutti sitä. NetOp RC –ohjelmistosta ja sen käyttämästä protokollasta saimme materiaalia sähköpostitse. Yhteyshenkilönä meillä oli Jukka Stenius, joka työskentelee NetOp Finland Oy:ssä. Motivaation puute koski lähinnä viitekehyksen kirjoittamista ja työn loppuun saattamista. Käytännön osuus sen sijaan oli erittäin mielenkiintoinen prosessi.

Emme osallistuneet kovinkaan moniin seminaareihin tai ohjaustilaisuuksiin, joten palautetta kyseisen työn tiimoilta ei paljoa tullut koululta tai opettajilta. Onneksi Yritys X:n it-vastaava oli erittäin mukava ja auttavainen henkilö, sillä hän käytännössä ohjasi prosessia eteenpäin. Työn viivästyminen aiheutti myös muitakin seurauksia, kuin valmistumisen lykkäytymisen, sillä käytännössä kaikki kerätty materiaali on vuosilta 2007 ja 2008.

Työnjako oli melko tasaista siihen saakka, kunnes työparini päätti lopettaa koulun. Tämän jälkeen oma suorittaminen tuntui ajoittain mahdottomalta ja työ lojui laatikon pohjalla pitkiäkin aikoja.

LÄHTEET

Painetut lähteet

Ciscon verkkoakatemia : 1. vuosi. Helsinki : Edita, IT Press.

Kanter J.P. 1998. Thin-Client/Server Computing. Washington: Microsoft Press

Minasi, M., Anderson, C., Beveridge, M., Callahan, C.A. & Justice, L. 2003. Windows Server 2003. Sybex Inc.

Lamminmäki, S. & Hannus, J. 1993. Avoimet ja hajautetut tietojärjestelmät – Arkkitehtuurit, teknologia, välineet. Sivut 11, 31, 33. Jyväskylä: Gummerus Kirjapaino Oy.

Elektroniset lähteet

Authenticationworld: The Business of Authentication [www] Viitattu 14.2.2008 Saatavissa: http://www.authenticationworld.com/

Cygate: Autentikointi – todentaminen [www] Viitattu 14.3.2008 Saatavissa: http://www.cygategroup.com/templates/page.aspx?id=1466

MSDN: Remote Desktop Protocol [www]. Microsoft Corporation, 2007, päivitetty 2.7.2007 [Viitattu 27.8.07]. Saatavissa:
http://msdn2.microsoft.com/en-us/library/Aa383015.aspx

RealVNC: The RFB Protocol [www]. RealVNC Ltd, 2002, päivitetty 18.7.2007 [Viitattu 03.09.2007]. Saatavissa: http://www.realvnc.com/docs/rfbproto.pdf

RSA Labotories: AES Algorithm [www]. RSA Labotories 2007 [Viitattu 6.2.2008] Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2235

RSA Labotories: DES Algorithm [www]. RSA Labotories 2007 [Viitattu 6.2.2008] Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2226

RSA Labotories: Diffie-Hellman [www]. RSA Labotories 2007 [Viitattu 11.2.2008] Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2248

RSA Labotories: Hash functions [www]. RSA Labotories 2007 [Viitattu 7.2.2008] Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2176

RSA Labotories: RC4 Algorithm [www]. RSA Labotories 2007 [Viitattu 6.2.2008] Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2250

RSA Labotories: RSA Algorithm [www]. RSA Labotories 2007 [Viitattu 3.10.2007] Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2146

Sanastokeskus TSK: asiakaskone; asiakas [www]. Sanastokeskus, päivitetty 13.10.2000 [Viitattu 7.2.2008]. Saatavissa:
http://www.tsk.fi/termitalkoot/search.php?page=get_id&id=ID0083&vocabulary_code=TSKTT

SearchWinIT.com: Face-off: Thin clients vs. fat clients [www]. Päivitetty 8.1.2004. [Viitattu 7.2.2008] Saatavissa:
http://searchwinit.techtarget.com/news/article/0,289142,sid1_gci943333,00.html

Stenius, Jukka. VS:NetOp Remote Control 9.0. Sähköpostiviesti. Vastaanottaja: Toni Hannula. 6.10.2008

Ståhlberg M. ja Uskela S.: Nykyisiä tiedon suojaus menetelmiä [www]. Helsingin teknillinen korkeakoulu, Sähkö- ja tietoliikennetekniikan osasto, 1998. päivitetty 27.11.1998 [Viitattu 22.8.2007]. Saatavissa:
http://www.netlab.tkk.fi/opetus/s38118/s98/htyo/1/hyss_3.shtml

Taimila L.: Ohuet asiakassovellukset ohjelmistoteknisestä näkökulmasta [www]. Taimila [2.10.2007] Saatavissa: http://www.taimila.com/files/luk-tutkielma.pdf

Tietotekniikan liitto ry.: Palvelintekniikka [www] Tietotekniikan liitto ry, 2004, päivitetty 8.3.2004 [Viitattu 6.2.2008]. Saatavissa:
http://www.ttlry.fi/yhdistykset/osaamisyhteisot/atk-sanasto/viikon_sana/?x20547=24338

Tietotekniikan liitto ry: yhteyskäytäntö [www]. Tietotekniikan liitto Ry, päivitetty 2007 [Viitattu 15.2.2008]. Saatavissa:
http://www.ttlry.fi/atk-sanakirja/su026.htm#5388

Tilastokeskus: Krypton salat ja tilastotiede [www]. Tilastokeskus, päivitetty 21.04.2005. [Viitattu 22.8.2007]. Saatavissa:
http://www.stat.fi/tup/tietoaika/tilaajat/ta_03_05_teikari.html

Unixwiz.net - Software Consulting Centeral: An Illustrated Guide to Cryptographic Hashes [www]. Päivitetty 9.5.2005 [Viitattu 7.2.2008] Saatavissa:
http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Viestintävirasto: Salausmenetelmät [www]. Viestintävirasto, 2006, päivitetty 27.09.2007. [Viitattu 22.8.2008]. Saatavissa:
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html

Viestintävirasto: Symmetrinen salaus [www]. Viestintävirasto, 2006, päivitetty 27.09.2007. [Viitattu 22.8.2008]. Saatavissa:
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/symmetrinensalaus.html

Viestintävirasto: Epäsymmetrinen salaus [www]. Viestintävirasto, 2006, päivitetty 27.9.2007. [Viitattu 22.8.2008]. Saatavissa:
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/epasymmetrinensalaus.html

Ote UltraVNC-ohjelman salaamattomasta liikenteestä LIITE 1

No. Time Source Destination Protocol Info
4 2.639926 192.168.1.4 192.168.1.5 TCP 4276 > 5900 [SYN] Seq=0 Len=0 MSS=1460

Frame 4 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Msi_78:31:35 (00:16:17:78:31:35), Dst: Microsof_79:31:35 (00:03:ff:79:31:35)
Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 192.168.1.5 (192.168.1.5)
Transmission Control Protocol, Src Port: 4276 (4276), Dst Port: 5900 (5900), Seq: 0, Len: 0

No. Time Source Destination Protocol Info
5 2.641325 192.168.1.5 192.168.1.4 TCP 5900 > 4276 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

Frame 5 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Microsof_79:31:35 (00:03:ff:79:31:35), Dst: Msi_78:31:35 (00:16:17:78:31:35)
Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: 5900 (5900), Dst Port: 4276 (4276), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
6 2.641600 192.168.1.4 192.168.1.5 TCP 4276 > 5900 [ACK] Seq=1 Ack=1 Win=65535 Len=0

Frame 6 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: Msi_78:31:35 (00:16:17:78:31:35), Dst: Microsof_79:31:35 (00:03:ff:79:31:35)
Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 192.168.1.5 (192.168.1.5)
Transmission Control Protocol, Src Port: 4276 (4276), Dst Port: 5900 (5900), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
7 2.647207 192.168.1.5 192.168.1.4 VNC Server protocol version: 003.006

Frame 7 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Microsof_79:31:35 (00:03:ff:79:31:35), Dst: Msi_78:31:35 (00:16:17:78:31:35)
Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: 5900 (5900), Dst Port: 4276 (4276), Seq: 1, Ack: 1, Len: 12
Virtual Network Computing
Server protocol version: 003.006

Ote UltraVNC-ohjelman salatusta liikenteestä LIITE 2

Frame 8 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Msi_78:31:35 (00:16:17:78:31:35), Dst: Microsof_79:31:35 (00:03:ff:79:31:35)
Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 192.168.1.5 (192.168.1.5)
Transmission Control Protocol, Src Port: 4275 (4275), Dst Port: 5900 (5900), Seq: 0, Len: 0

No. Time Source Destination Protocol
Info
9 9.440121 192.168.1.5 192.168.1.4 TCP 5900 > 4275 [SYN, ACK] Seq=0
Ack=1 Win=65535 Len=0 MSS=1460

Frame 9 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Microsof_79:31:35 (00:03:ff:79:31:35), Dst: Msi_78:31:35 (00:16:17:78:31:35)
Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: 5900 (5900), Dst Port: 4275 (4275), Seq: 0, Ack: 1,
Len: 0

No. Time Source Destination Protocol
Info
10 9.440397 192.168.1.4 192.168.1.5 TCP 4275 > 5900 [ACK] Seq=1
Ack=1 Win=65535 Len=0

Frame 10 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: Msi_78:31:35 (00:16:17:78:31:35), Dst: Microsof_79:31:35 (00:03:ff:79:31:35)
Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 192.168.1.5 (192.168.1.5)
Transmission Control Protocol, Src Port: 4275 (4275), Dst Port: 5900 (5900), Seq: 1, Ack: 1,
Len: 0

No. Time Source Destination Protocol
Info
18 22.450829 192.168.1.5 192.168.1.4 VNC Server protocol version:
\207w-\177\235C:

Frame 18 (93 bytes on wire, 93 bytes captured)
Ethernet II, Src: Microsof_79:31:35 (00:03:ff:79:31:35), Dst: Msi_78:31:35 (00:16:17:78:31:35)
Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: 5900 (5900), Dst Port: 4275 (4275), Seq: 1, Ack: 1,
Len: 39
Virtual Network Computing
Server protocol version: \207w-\177\235C:

Etäkäyttöohjelmien ominaisuudet LIITE 3/1

Ohjelma	Etätyöpöytäyhteys
Ohjelma versio	6.0 (6.0.6000)
Protokolla versio	RDP
Käyttäjän tunnistus (Autentikointi)	Windowsin käyttäjätilit
Yhteyden salaus	RC4 128bit
Manuaalinen yhteyden varmennus	Ei
Kuvan näyttö palvelimella etäkäytön aikana	Ei
Tiedostojen siirto	Ei
Tekstipohjainen keskustelu	EI
Palvelimen käyttämät portit	3389
Selainpohjainen käytettävyys	Ei
Tuetut käyttöjärjestelmät	Win XP Pro ja Terminal Server
Windows Vista tuki	Kyllä
Kieli	Englanti ja suomi
Hinta	Ilmainen

Ohjelma	NetOp
Ohjelma versio	9.0 (2007250)
Protokolla versio	DTL (Danware Transport Layer)
Käyttäjän tunnistus (Autentikointi)	2048bit DH76
Yhteyden salaus	256bit AES ja HMAC 160bit SHA-1 tai 256bit SHA-256
Manuaalinen yhteyden varmennus	Kyllä
Kuvan näyttö palvelimella etäkäytön aikana	Kyllä.
Tiedostojen siirto	Kyllä.
Tekstipohjainen keskustelu	Kyllä.
Palvelimen käyttämät portit	6502
Selainpohjainen käytettävyys	Asiakas ohjelmassa ActiveX tuki.
Tuetut käyttöjärjestelmät	Win9x/NT/Me/2000/XP/2003/Terminal Server. Rajoitettu toimivuus Win CE, Linux, Solaris, Symbian OS ja ActiveX
Windows Vista tuki	Kyllä
Kieli	englanti ja suomi
Hinta	1 kpl asiakas 140€ ja 100 kpl palvelin 4370€

LIITE 3/2

Ohjelma	RealVNC
Ohjelma versio	4.3.2
Protokolla versio	VNC 4.0
Käyttäjän tunnistus (Autentikointi)	VNC 2048 bittinen RSA ja paikallinen/ toimialue
Yhteyden salaus	128 bittinen AES
Manuaalinen yhteyden varmennus	Kyllä
Kuvan näyttö palvelimella etäkäytön aikana	Kyllä
Tiedostojen siirto	Kyllä. Leikepöydän kautta
Tekstipohjainen keskustelu	Ei.
Palvelimen käyttämät portit	5900
Selainpohjainen käytettävyys	Kyllä
Tuetut käyttöjärjestelmät	Win9x/Me/NT4/2000/XP/2003
Windows Vista tuki	Kyllä.
Kieli	Englanti
Hinta	1 palvelin / 33.81 € 100 palvelinta / 1176.83 €

Ohjelma	TeamViewer
Ohjelma versio	3.0.3793
Protokolla versio	-
Käyttäjän tunnistus (Autentikointi)	1024bit RSA
Yhteyden salaus	128bit RC4
Manuaalinen yhteyden varmennus	Ei.
Kuvan näyttö palvelimella etäkäytön aikana	Kyllä.
Tiedostojen siirto	Kyllä.
Tekstipohjainen keskustelu	Kyllä.
Palvelimen käyttämät portit	5938. Ei mahdollisuutta vaihtaa,
Selainpohjainen käytettävyys	Ei.
Tuetut käyttöjärjestelmät	Win98/ME/NT/2000/XP/2003
Windows Vista tuki	Kyllä.
Kieli	Englanti
Hinta	1 client 499 € / +1 client 99 €

LIITE 3/3

Ohjelma	TightVNC
Ohjelma versio	1.3.9
Protokolla versio	3.8tight
Käyttäjän tunnistus (Autentikointi)	VNC autentikointi (DES)
Yhteyden salaus	Ei
Manuaalinen yhteyden varmennus	Kyllä
Kuvan näyttö palvelimella etäkäytön aikana	Kyllä.
Tiedostojen siirto	Kyllä
Tekstipohjainen keskustelu	Ei.
Palvelimen käyttämät portit	5900
Selainpohjainen käytettävyys	Kyllä
Tuetut käyttöjärjestelmät	Win9x/Me/NT4/2000/XP/2003 ja Linux/Unix
Windows Vista tuki	Ei.
Kieli	Englanti
Hinta	Ilmainen

Ohjelma	UltraVNC
Ohjelma versio	1.0.2
Protokolla versio	VNC 3.6
Käyttäjän tunnistus (Autentikointi)	VNC, paikallinen käyttäjätili tai toimialue
Yhteyden salaus	128 bit RC4 ja 128 bit AES
Manuaalinen yhteyden varmennus	Kyllä
Kuvan näyttö palvelimella etäkäytön aikana	Kyllä. Mahdollista estää.
Tiedostojen siirto	Kyllä.
Tekstipohjainen keskustelu	Kyllä.
Palvelimen käyttämät portit	5900.
Selainpohjainen käytettävyys	Kyllä
Tuetut käyttöjärjestelmät	Win9x/Me/NT4/2000/XP/2003
Windows Vista tuki	Tulossa.
Kieli	Englanti
Hinta	Ilmainen