Tytti Kurtti, Hannakaisa Isomäki, Kimmo Kokkonen
Kirsi Päykkönen, Hanna Räisänen

Langattoman opiskelu-ympäristön tietoturva

Raportti opetuskokeilusta

Lapin yliopiston menetelmätieteiden laitos
Soveltavan informaatioteknologian yksikkö

Lapland University Press
Lapin yliopistokustannus
www.ulapland.fi/unipub

Rovaniemi 2007

ISBN 978-952-484-086-6

Tytti Kurtti, Hannakaisa Isomäki, Kimmo Kokkonen, Kirsi Päykkönen, Hanna Räisänen

Langattoman opiskeluympäristön tietoturva

Raportti opetuskokeilusta
Lapin yliopisto 2007

Tiivistelmä

Langattoman opiskeluympäristön tietoturva -opetuskokeilu käynnistettiin Lapin yliopistossa syksyllä 2006. Hankkeen rahoitti Opetuksen kehittämispalvelut. Opetus toteutettiin sekä lähiopetuksena että verkko-opetuksena. Hankkeen tuotoksiin kuuluu muun muassa tämä raportti.

Raportin tarkoituksena on toimia ohjeistuksena langattoman kampuksen verkko-opetusta suunnitteleville opettajille sekä opiskelijoille. Siinä käydään läpi verkko-opiskeluun, langattomaan tietoverkkoon sekä tietoturvaan liittyviä asioita. Lapin yliopiston langaton kampus on toiminut jo muutaman vuoden. Opiskelijat käyttävät yliopiston tarjoamia kannettavia tietokoneita opiskelussaan, jolloin tietoturvan merkitys korostuu. Raporttiin on koottu opetuskokeiluun sisältyvän kurssin opetusmateriaali sekä opiskelijapalaute.

Asiasanat: langaton verkko, verkko-opiskelu, opiskeluympäristö, tietoturva

Sisällysluettelo

1 Johdanto

Tietoturvan merkitys on korostunut tietotekniikan hyödyntämisen sekä langattomien tietoverkkojen yleistymisen myötä. Myös koulutuksessa hyödynnetään nykyisin yhä enemmän tietokoneita, erilaisia tietoverkkopohjaisia opiskeluympäristöjä sekä muita informaatioteknologian apuvälineitä. Lapin yliopiston opiskelijoilla on mahdollisuus käyttää kannettavia tietokoneita sekä langatonta verkkoa. Uudet opiskelijat ovat saaneet yliopistolta käyttöönsä pientä maksua vastaan oman kannettavan tietokoneen syksystä 2004 alkaen. Suurin osa uusista opiskelijoista on ottanut kannettavan tietokoneen vastaan. Syksyllä 2004 uusista opiskelijoista 561 otti kannettavan vastaan. Syksyllä 2005 vastaava luku oli 537 ja syksyllä 2006 uusista opiskelijoista 481 vastaanotti kannettavan tietokoneen.

Osa opiskelusta toteutetaan verkko-opiskeluympäristössä. Tällöin tietoturvan merkitys korostuu, sillä suuria määriä tietoaineistoja välitetään verkon välityksellä. Nykyisin Lapissa on kiinnitetty erityistä huomiota tietoturvan kehittämiseen. Rovaniemen tietoturvaklusteri perustettiin vuonna 2004 ja sen tarkoituksena on toimia tietoturva-alan osaamiskeskittymänä kehittäen tietoturva-alan tutkimusta ja koulutusta.

Langattoman opiskeluympäristön tietoturva -opetuskokeilun raportin tarkoituksena on pohtia langattoman tietoturvan merkitystä verkko-opiskeluympäristössä. Tämä raportti toimii oppaana langattomaan verkkoon pohjautuvaa opetusta suunnitteleville ja käyttäville henkilöille. Tarkoituksena on, että opettaja pystyy toimimaan langattomassa opiskeluympäristössä siten, että käytössä olevat tietoturvatavoitteet otetaan huomioon opetuksessa. Raportissa tarkastellaan muun muassa verkko-opetusmateriaalia ja sen kriteerejä tietoturvan näkökulmasta, langattoman verkko-opiskeluympäristön tietoturvaa sekä välitetään opiskelijoiden kokemuksia toteutuneen opetuskokeilun pohjalta.

Opetuskokeilussa tarkastelun kohteena ovat muun muassa seuraavat asiat:

1. Mitkä ovat tietoturvan kannalta keskeiset asiat verkkokurssien suunnittelussa ja toteutuksessa silloin, kun opetus, opiskelu ja oppiminen tapahtuvat langattomassa verkko-opiskeluympäristössä?
2. Tietoturvaominaisuuksien käytön opettelu
3. Langattomien tietoliikenneverkkojen tietoturva
4. Mitä vaatimuksia kurssien toteuttaminen langattomassa verkko-opiskeluympäristössä asettaa tietoturvalle ja tietosuojalle?

Langattoman opiskeluympäristön tietoturva -opetuskokeilu käynnistyi Lapin yliopistossa syksyllä 2006. Hankkeessa toteutettiin kurssi SOIT1305 Langattoman opiskeluympäristön tietoturva. Kurssi koostuu neljästä toisiaan tukevasta luento-osuudesta, opiskelijoiden keskusteluosuudesta sekä opiskelijoiden käyttöpäiväkirjoista. Hankkeen tuotoksiin kuuluu myös tämä raportti. Hankkeen rahoitti Lapin yliopiston Opetuksen kehittämispalvelut.

Opetuskokeilun taustalla oli projekti, johon osallistuivat opetuskokeilun opettajat. Vastuullisena johtajana toimi Soveltavan informaatioteknologian professori Hannakaisa Isomäki. Kokeilu eteni vaiheittain ja kokonaisuuteen kuului suunnittelu, toteutus sekä arviointi. Suunnitteluun osallistuivat opetuskokeilun opettajat. Toteutusvaiheessa järjestettiin neljästä luento-osuudesta koostunut lähiopetus sekä opiskeluympäristön

hallinta. Opetusmateriaali koottiin tähän raporttiin ja kurssin opettajat tarkastivat materiaalin ennen raportin julkistamista. Raportin kirjoitti Tytti Kurtti.

Opettajina kurssilla toimivat seuraavat henkilöt: soveltavan informaatioteknologian tutkimusassistentti Kirsi Päykkönen, tietotekniikan lehtori Hanna Räisänen, informaatioteknologian päätoiminen tuntiopettaja Kimmo Kokkonen sekä Hannakaisa Isomäki. Kirsi Päykkönen perehdytti opiskelijat aluksi tietoturvan perustoimintoihin ja niiden käyttöön. Hanna Räisänen luennoi tietoturvallisesta yhteisöllisestä opiskelusta ja verkkokurssien suunnittelusta. Kimmo Kokkonen perehdytti opiskelijat langattomien tietoverkkojen tietoturvaan eli hänellä oli vastuullaan tekniseen tietoturvaan liittyvät asiat. Hannakaisa Isomäki päätti lähiopetusosuuden luennollaan tietoturva, oikeusinformatiikka ja käyttöliittymät. Jokaisen opettajan luentoon kuului myös keskustelutehtävä. Opetus toteutettiin Discendum Optima -verkko-opiskeluympäristössä. Opetuskokeiluun osallistui yksi yhteiskuntatieteiden tiedekunnan ja kuusi kasvatustieteiden tiedekunnan opiskelijaa.

2 Verkko-opiskelu ja -opiskelumateriaali opiskeluympäristössä

Lapin yliopistossa verkko-opetusta on tarjottu jo pitkään, mutta langattoman verkon kautta tapahtuva opiskelu on aloitettu vuodenvaihteessa 2004–2005, jolloin kampukselle asennettiin langaton lähiverkko. Kannettavien tietokoneiden myötä verkko-opiskelusta on tullut helpompaa ja nopeampaa, jolloin opiskelu yliopiston tiloissa on muuttunut opiskelijalähtöiseksi.

Lapin yliopistossa käytetään Discendum Optima -verkko-opiskeluympäristöä. Verkko-opiskelu vaatii sekä opettajalta että opiskelijalta kykyä oppia uusia opiskelu- ja opetusmuotoja, jotta verkko-opiskelua voidaan hyödyntää monipuolisesti. Tässä luvussa tarkoituksena on kartoittaa, miten verkko-opiskelun kehitys on edennyt ja mitä opetushenkilöstön kannattaa huomioida järjestäessään verkko-opetusta. Luvussa viitataan Mäkiseen (2006), Kallialaan (2002), Sariolaan (2003), Silanderiin ja Koliin (2003), teokseen Yliopisto-opetus ja oppiaineisto verkossa (1999) sekä verkkoaineistoon Opetusministeriön laatukriteerit (www.edu.fi/julkaisut/laatukriteerit.pdf).

2.1 Verkko-opiskelu

Verkko-opiskelu tarkoittaa tietoverkkojen välityksellä tapahtuvaa aikaan ja paikkaan sitoutumatonta opiskelua. Tietoverkot voivat toimia koulutusmateriaalin jakelukanavana ja niitä voidaan hyödyntää oppimisprosessiin osallistuvien yhteisenä toiminta- ja vuorovaikutusympäristönä. Kyse on ihmisten välisestä vuorovaikutuksesta, jossa tietokone toimii välittäjänä. Verkko-opiskelu voi myös täydentää lähiopiskelua. Yhä useammin verkko on yksi mahdollinen opiskelumuoto kokonaisvaltaisessa opiskelussa.

Verkko-opiskelu on osittain verkkokoulutuksen tulosta ja osittain koulutuksesta riippumatonta omatoimista, tietoverkkoon tukeutuvaa oppimista. Verkko-opiskelua voidaan luonnehtia sen mukaan, miten aika ja paikka yhdistetään opiskelussa:

1. verkon tukema lähiopetus (sama aika ja sama paikka)
2. monimuoto-opetus verkossa (eri aika ja eri paikka paitsi yhteisten tapaamisten aikana)
3. itseopiskelu verkossa.

Edellä mainittujen verkko-opiskelumuotojen rajat ovat häilyviä ja yleensä verkkokurssit ovatkin eri opiskelumuotojen yhdistelmiä, pääasiassa monimuoto-opetusta. Tällöin lähiopetuksen määrä vähenee tai ne toteutetaan videoneuvotteluina. Opettajan rooli verkossa on opettamisen ohessa ohjaaja, tutkija, opastaja, kysymyksiin vastaaja, ongelmatilanteiden selvittäjä ja palautteen antaja. Verkko-opiskelun toteuttamisessa edellytetään yleensä toimivia verkkovuorovaikutuksen mahdollisuuksia, kuten sähköpostia, chat-ryhmiä, muita keskusteluryhmiä sekä ryhmätyön edellyttämiä mahdollisuuksia.

Verkko-opiskelua ja sen eri muotoja on kutsuttu erilaisilla termeillä. 1980-luvulla puhuttiin tietokoneavusteisesta oppimisesta (TAO), mistä ovat peräisin tietoverkko-opiskelu, e-opiskelu (elektroninen opiskelu) sekä nykyisin yleisimmin käytetty termi verkko-opiskelu. Joskus mainitaan myös virtuaaliopiskelu, mutta sen määrittely on koettu liian hankalaksi.

Mobiiliopiskelu eli m-opiskelu on uusin opiskelumuoto, joka tarkoittaa opiskelua erilaisten mobiilisovellusten avulla. Mobiilisuudella tarkoitetaan muun muassa vapaata liikkuvuutta, nopeaa liikuteltavuutta sekä muuttuvuutta, joten opiskelu ei ole enää aikaan ja paikkaan sidottua. Mobiilisuus tuo opiskeluun joustavuutta sekä edistää tavoitettavuutta ja viestintää. Mobiiliopiskelun välineitä ovat muun muassa kannettava tietokone, kommunikaattori tai kämmentietokone eli PDA (Personal Digital Assistant).

2.2 Opetusmateriaali verkko-opiskeluympäristössä

Verkko-opiskelumateriaali tarkoittaa opettajan laatimaa materiaalia verkkoon. Näitä ovat muun muassa kurssikuvaus, kurssin tehtävät, ohjeistus, lähiopetuksessa esitetyt kalvot, kalvojen mahdolliset tausta-aineistot tai opettajan laatima verkkokirja tai muu kirjallinen tuotos. Verkkomateriaali voi olla myös opiskelijoiden verkko-opiskeluympäristössä tuottama verkkomateriaali.

Verkko mahdollistaa etäopetuksen, jolloin pelkästään lähiopetuksessa käytettävän oppimateriaalin lisäksi verkkoon siirretään myös opetus ja opiskeluprosessin ohjaus. Monet verkko-opiskelumateriaaleista ovat kokonaisuuksia kursseista jotka koostuvat oppimateriaaleista ja verkossa tapahtuvasta vuorovaikutuksesta. Opetusaineisto on tavallaan sekä materiaalissa että ihmisten välisessä vuorovaikutuksessa ja opetusmateriaalin todellinen laatu tulee ilmi vasta käytössä ja kontekstissa.

Opiskelumateriaali kannattaa tehdä rakenteiseksi, jotta materiaalin sisältö, rakenne ja ulkoasu eivät olisi riippuvaisia toisistaan. Tällöin materiaali pysyy rakenteeltaan samana, vaikka sen ulkoasu eri päätelaitteilla vaihtelisi. Digitaalisessa muodossa olevaa opetusmateriaalia on helppo muokata ja päivittää.

Verkko-opiskelun keskeisimpiä tavoitteita on vuorovaikutuksellinen opiskelu. Vuorovaikutus tarkoittaa prosessia, josta löytyvät viestin lähettäjä, viestin vastaanottaja sekä viestintäkanava, jota myöten viesti etenee lähettäjältä vastaanottajalle. Verkko-opiskelussa vuorovaikutuksen onnistumiseen vaikuttavat seuraavat asiat:

- viesti on lähetetty vastaanottajalle ymmärrettävässä muodossa
- joku vastaanottaa viestin
- vastaanottaja ymmärtää viestin lähettäjän tarkoittamassa merkityksessä
- vastaanottaja reagoi viestiin.

Verkko-opiskelun vuorovaikutuksellisuus ilmenee selkeimmin verkko-opetusympäristön keskustelualueella. Verkkokeskustelun katsotaan edistävän yhteisöllistä opiskelua, jolloin opiskelijat voivat keskenään kehittää ja ideoida opiskeltavaa aihealuetta keskustelun avulla. Verkkokeskustelun etuihin kuuluu kaikkien opiskelijoiden mahdollisuus osallistua keskusteluun, miettimisaikaa ja harkintaa vaativien tehtävien tiedonrakentelu, keskustelujen dokumentoituminen sekä verkkokeskusteluosaamisen kehittyminen. Verkkokeskustelussa opiskelija joutuu ulkoistamaan omia ajatuksiaan sekä reflektoimaan niitä toisten opiskelijoiden ajatuksiin. Opiskelijat kokevat lisäksi yhdessä ajattelemista, mistä käytetään termiä sosiaalisesti hajautettu kognitio. Opiskelija voi myös jälkeenpäin tarkastella ulkoistettua ongelmanratkaisu- tai ajatteluprosessia ja oppia siitä. Verkkokeskustelun aiheita voivat olla muun muassa itsensä esittely, erilaisten ongelmien ja kysymysten asettaminen, omien selitysten esittely, muiden

käsityksiin tutustuminen ja niiden kommentointi, kysymysten esittäminen, opiskelun organisointiin liittyvät asiat tai palautteenanto.

2.3 Verkko-opiskelumateriaalin laatukriteerit tietoturvallisuuden näkökulmasta

Verkkoon vietävän opetusmateriaalin tulee täyttää tietoturvallisuuden vaatimukset. Verkko-opiskelumateriaalin ominaispiirteisiin kuuluvat päivitettävyys, vuorovaikutteisuus sekä yhteisöllisyys. Verkko mahdollistaa opiskelumateriaalin laajemman käytön. Uuden jakelukanavan myötä materiaali on usean henkilön käytettävissä. Keskeisimmät muutokset tapahtuvat kuitenkin seuraavien asioiden osalta: vuorovaikutteisuuden huomioiminen, kontekstin huomioon ottaminen, soveltuvuus oman opetuksen ulkopuolella, tekijänoikeudet ja käyttöoikeudet.

Opetushallitus on asettanut verkko-opiskelumateriaalille yleisiä laatukriteereitä. Nämä ovat:

- pedagoginen laatu
- käytettävyys
- esteettömyys
- tuotannon laatu

Pedagoginen laatu tarkoittaa opiskelumateriaalin soveltuvuutta luontevasti opetus- ja opiskelukäyttöön. Lisäksi opiskelumateriaali on tuettava opetusta ja opiskelua ja tarjottava pedagogista lisäarvoa. Opiskelumateriaalin soveltuvuus on yhteydessä käyttötilanteeseen, opiskelijoiden odotuksiin sekä osaamiseen. Opiskelumateriaalin on tuettava oppimista ja tuotava opiskeluun lisäarvoa huomioimalla opiskelijan taitojen merkityksellisyys ja aktiivisuus opeteltavan asian suhteen sekä opiskelutehtävien haasteellisuus, avoimuus sekä merkityksellisyys ja aitous opiskelijan kannalta.

Käytettävyys kuuluu tietoturvan tavoitteisiin. Opiskelumateriaalin osalta käytettävyydellä tarkoitetaan materiaalin rakenteen, teknisen toteutuksen ja käyttöliittymäsuunnittelun tuottamaa käytön sujuvuutta ja helppoutta. Heikko käytettävyys voi aiheuttaa käyttäjän turhautumista tietojen etsimisessä tai työskentelyssä esimerkiksi virheilmoituksien, toimimattomien linkkien, epäselvien ilmaisujen tai ohjeiden puutteiden seurauksena. Verkko-opetusmateriaalin tekijälle käytettävyyden tulee olla yksi tuotannon perustavoitteista ja jatkuvan varmistuksen kohde.

Esteettömyydellä tarkoitetaan sitä, että opiskelumateriaali on käytettävissä riippumatta ihmisen fyysisistä ja psyykkisistä ominaisuuksista, vammoista ja terveydentilasta. Esteettömyyskriteerit ovat monessa suhteessa samansuuntaisia kuin käytettävyyskriteerit. Esteettömyyskriteerit on tarkoitettu sovellettaviksi ottaen huomioon opiskelumateriaalille asetettavat tavoitteet. Käytännössä esteettömyystavoitteita joudutaan rajaamaan tai ne rajautuvat sen mukaan, mikä on mahdollista, kun otetaan huomioon muut tavoitteet, verkko-opetusmateriaalin kohderyhmä ja käytettävissä olevat voimavarat. Jos esteettömyystavoitteista tingitään, tulisi kuitenkin huolehtia siitä, että haitat ja ongelmat ovat mahdollisimman vähäisiä.

Tuotannon laatu muodostuu hallitusti toteutetusta tuotantoprosessista, jota ohjaavat tiedolliset, taidolliset ja oppimista ohjaavat tavoitteet. Tuotannon on oltava pedagogisesti laadukasta ja sen on täytettävä sekä käytettävyyden että esteettömyyden vaatimukset. Tuotannon laadussa huomioidaan myös käyttäjäryhmät, käyttäjien tarpeet ja

käyttötilanteet. Lisäksi verkko-opiskelumateriaalin suunnittelu- ja tuotantoprosessissa painotetaan käyttäjänäkökulmaa, jolloin käyttäjien edustajia osallistuu verkko-opiskelumateriaalin tuottamiseen ja tuotetta testataan pilottikäytöllä. Verkko-opiskelumateriaalia tuotettaessa on hallittava tekijän- ja käyttöoikeuksia eli opettajan on noudatettava tietosuojan vaatimuksia ja tekijänoikeuslainsäädäntöä. Tuotannon laadussa varmistetaan myös verkko-opiskelumateriaalin turvallisuus ja tekninen toimivuus.

Verkkoon tuotetussa opiskelumateriaalissa täytyy huomioida tekijänoikeussuoja. Yliopistossa tuotettu materiaali on tekijänoikeudella suojattu. Näitä ovat muun muassa luentomonisteet ja -kalvot, tenttikysymykset, tekstiin liittyvät piirustukset ja kaaviot sekä kuvat. Tekijänoikeudella suojattuja eivät puolestaan ole esimerkiksi uusi tapa opetuksen tuottamisessa verkon välityksellä, keksinnöt (suojataan erikseen patentilla), tietyn kurssin tietosisältö, matemaattiset yhtälöt sekä kaavamaiset ilmaisut.

Yliopisto-opettajalla on vakiintuneen käytännön mukaisesti tekijänoikeudet tekemiinsä tutkimuksiin ja oppimateriaaleihin. Opettajan valmistamaa materiaalia yliopisto ei voi käyttää ilman opettajan lupaa. Verkkomateriaalissa sovelletaan työsuhdetekijänoikeuden yleisiä periaatteita. Jos yliopisto on antanut opettajalle tehtäväksi verkkoon tuotetun opetusmateriaalin valmistamisen, yliopistolle siirtyy materiaaliin liittyvät normaalissa toiminnassa tarvittavat tekijänoikeudet. Jos opettaja tekee yliopiston kanssa sopimuksen, että hän valmistelee ja toteuttaa opetuksensa verkon välityksellä ja verkkoon valmistetaan opetusmateriaalia, yliopisto saa vähintään rinnakkaisen käyttöoikeuden aineistoon. Tähän on syynä se, että opetusmateriaali on tehty virkasuhteessa siinä tarkoituksessa, että yliopisto voi käyttää sitä tarkoittamallaan tavalla.

Myös opiskelija voi tuottaa aineistoa verkkoon esimerkiksi lähettämällä harjoitustyön, esseen tms. verkko-opiskeluympäristöön. Tällöin olisi hyvä sopia, missä laajuudessa yliopisto voi hyödyntää opiskelijan tuottamaa materiaalia. Opiskelija osallistuu opiskelumateriaalin luomiseen, jos hänen tuotoksensa yhdistetään muiden aineistoon, jota esimerkiksi kurssille osallistuvat henkilöt voivat lukea. Opiskelijalla on myös vastuu aineistonsa lähteistä eli hänen tulee noudattaa aineistonsa suhteen muita tekijänoikeusvaatimuksia. Opiskelijan tuottamaa aineistoa ei voida kuitenkaan hyödyntää ilman opiskelijan lupaa.

3 Langaton verkko-opiskeluympäristö ja tietoturva

Lapin yliopiston opiskelijoilla on mahdollisuus hyödyntää yliopistokampuksen langatonta verkkoyhteyttä. Verkko-opiskeluympäristöillä tarkoitetaan sähköisesti luotuja virtuaalisia tiloja verkossa, joissa mahdollistuu luokkahuonetta laajempi opiskelu. Erilaisia verkko-opiskeluympäristöjä ovat muun muassa Discendum Optima, Moodle sekä WebCT. Lapin yliopistossa opiskeluympäristönä käytetään Discendum Optima -verkko-opiskeluympäristöä.

Opiskelijat kirjautuvat verkko-opiskeluympäristöön omilla tunnuksilla ja salasanoilla ja he pystyvät osallistumaan ja hankkimaan informaatiota vain niiltä kursseilta, joita he suorittavat. Kurssin tietoaineistoon eivät pääse tutustumaan ulkopuoliset. Verkossa voi opiskella mihin aikaan vuorokaudesta tahansa, joten se on joustava opiskelumuoto. Langaton verkkoympäristö tarkoittaa sitä, että opiskelija voi kytkeä kannettavan tietokoneensa verkkoon ilman kaapeleita koneeseen asennetun langattoman verkkokortin avulla. Kannettavan tietokoneen tietoturvaan liittyvät asiat ovat opiskelijan omalla vastuulla. Näitä toimintoja ovat muun muassa varmuuskopiointi, virustorjuntaohjelmistojen päivittäminen sekä fyysinen vastuu tietokoneesta varastamisen ja vahingonteon osalta.

Seuraavassa perehdytään tarkemmin langattomaan verkkoon, tietoturvaan ja tietosuojaan sekä Lapin yliopistossa käytössä olevaan langattomaan lähiverkkoon sekä Optima-opiskeluympäristöön. Tässä kappaleessa viitataan Järviseen (2002), Kallialaan (2002), Magnusson-Sjöbergiin (2005) sekä Miettiseen (1999), Ruohoseen (2002) sekä Thomakseen (2005). Verkkolähteinä on käytetty seuraavia materiaaleja: Virtuaaliopetuksen haasteet ja niihin vastaaminen. (http://www.minedu.fi/OPM/Julkaisut/2002/virtuaaliopetuksen_haasteet_ja_niihin_vastaaminen?lang=fi/) sekä VAHTI- ja Tieke- tietoturvaohjeistuksia (http://www.vm.fi/vahti); (http://www.tieke). VAHTI- sivuilla on kattava esitys myös tietoturvaan liittyvästä lainsäädännöstä. Langattomaan verkkoon löytyy verkosta hyödyllisiä sivustoja kuten WLAN-Tietopankki: http://wlan.dacco.fi/sanasto.htm#wep/ ja MvNet: http://www.mvnet.fi/index.php?osio=Tietokoneet&sivu=Langaton_kotiverkko/.

3.1 Tietoturva

Tietoturva kattaa kaiken tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuden säilymiseen liittyvän käsittelyn, säilytyksen sekä tiedonsiirron aikana. Tietoturvaan liittyviä keskeisimpiä tavoitteita ovat luottamuksellisuus, eheys, saatavuus, todennus, pääsynvalvonta ja kiistämättömyys. Luottamuksellisuus tarkoittaa sitä, että tietoja käsittelevät vain ne henkilöt, jotka ovat siihen oikeutettuja. Luotettavuus varmistetaan salauksella, käyttöoikeuksien rajaamisella sekä valvonnalla. Eheys tarkoittaa tiedon pysymistä muuttumattomana. Tiedon on oltava ajanmukaista ja luotettavaa. Saatavuus tarkoittaa, että tieto on käytettävissä oikea-aikaisesti ja häiriöttä silloin, kun sitä tarvitaan.

Tietoturvallisuus perustuu Suomen lainsäädäntöön. Laki määrittelee tietoturvaan liittyviä määräyksiä ja toimintaohjeita. Lisäksi organisaatiot ovat laatineet omia

tietoturvaohjeistuksia varmistaakseen omassa toiminnassaan tietoturvallisen toimintakulttuurin.

Tietoturva muodostaa laajan asia-alueen ja sen vuoksi se on jaoteltu seuraaviin osa-alueisiin:

1. tietoaineiston turvallisuus
2. ohjelmistoturvallisuus
3. fyysinen turvallisuus
4. laitteistoturvallisuus
5. henkilöstöturvallisuus
6. käyttöturvallisuus
7. hallinnollinen turvallisuus

Tietoaineiston turvallisuus kattaa päivittäin käsiteltävien tietojen suojaamisen. Yleensä tietoaineiston turvallisuuden toteutus edellyttää tietojen turvaluokitusjärjestelmän, jossa kuvataan tietojen tarkoitus, tärkeys sekä se, miten tietoja käsitellään. Tietoaineiston turvallisuus takaa tietojen pysymisen asianosaisilla.

Ohjelmistoturvallisuus sisältää organisaation käyttämien tietokoneohjelmien lisensointiin ja rekisteröintiin liittyvät asiat. Ohjelmien sisäisiä suojausmenetelmiä ovat esimerkiksi ohjelmiston pääsynvalvonta, lokitietojen keruu sekä salasanojen automaattinen vanheneminen. Erillisiä suojausohjelmia ovat virustentorjuntaohjelmistot, tietojen ja tietoliikenteen salausohjelmistot sekä tietojen varmuuskopiointiohjelmistot.

Fyysinen turvallisuus kattaa organisaation toimintaympäristön turvallisuuden. Tällöin pyritään suojaamaan organisaation hallussa olevat toiminnassa tarvittavat tietoaineistot sekä fyysinen ja ei-fyysinen omaisuus tuhoutumiselta tai väärinkäytöltä. Esimerkiksi toimitilat ja niiden suojaamiseksi tarvittavat kulkuluvat ja murtosuojaukset kuuluvat tähän osa-alueeseen.

Laitteistoturvallisuus tarkoittaa tietojenkäsittely- sekä tietoliikennelaitteiden rakenteellista turvallisuutta. Laitteiden tulee olla toiminnaltaan varmoja sekä luotettavia. Laitteistoturvallisuus varmistetaan suunnittelussa, komponenttien valmistuksessa, laitteiden kokoonpanossa, varaosien suunnittelussa ja toteutuksessa sekä laitteiden kunnossapitoon liittyvien huolto- ja ylläpitorutiinien toteutuksessa.

Henkilöstöturvallisuus tarkoittaa henkilöihin liittyvän tiedon suojaamista sekä henkilöistä aiheutuvien uhkien estämistä. Henkilöstöturvallisuuteen lasketaan organisaation oman henkilöstön lisäksi toimintaan osallistuvat ulkopuoliset työntekijät sekä vierailijat. Yliopistossa henkilöturvallisuuteen kuuluvat myös opiskelijat. Henkilöstöturvallisuus korostuu uuden työntekijän rekrytoinnissa sekä työtehtävien vaihtuessa tai päättyessä. Henkilön taustatietojen tarkistaminen sekä työ- ja yhteistyösopimusten salassapito- ja vaitiolositoumukset ovat osa henkilöstöturvallisuutta.

Käyttöturvallisuus tarkoittaa päivittäisten käyttötoimintojen suojaamista. Näihin kuuluvat muun muassa käyttöoikeuksien määrittely, luominen, muuttaminen ja poistaminen. Käyttöturvallisuudella varmistetaan, että tietokone- ja tietoliikennelaitteita ylläpidetään ja hallitaan asianmukaisesti, käyttötoimintoja valvotaan ja dokumentoidaan asianmukaisesti sekä että kaikki toiminta tapahtuu sovittujen menettelytapojen mukaisesti.

Hallinnollinen turvallisuus sisältää tietoturvallisuuden toimintapolitiikan, linjaukset, johtamisen, resurssit, toimintojen organisoinnin ja sijoitukset sekä tietoturvallisuusasioiden hoitoon liittyvät vastuut.

Tietoturvan toteutumisessa keskeisessä osassa ovat ihmiset ja heidän käyttäytymisensä ja toimintatapansa.

3.2 Tietosuoja

Tietosuoja tarkoittaa henkilökohtaisten tietojen suojaamista esimerkiksi sähköisessä asioinnissa Internetissä. Tietosuoja tarkoittaa myös yksityisyyden suojaa. Yksityisyyden suoja kattaa ihmisen henkilötietojen sekä henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn henkilön yksityisyyttä vahingoittamattomalla tavalla. Luottamuksellisuuden varmistaminen sekä tekniset ja toiminnalliset järjestelyt tieturvallisuuden takaamiseksi vahvistavat myös tietosuojaa. Sähköisen viestinnän tietosuojalaki (SVTSL 516/2004) turvaa sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan sekä edistää sähköisen viestinnän tietoturvaa ja sähköisen viestinnän palvelujen kehittämistä.

Henkilökohtaisia tietoja käyttävien toimijoiden on huomioitava muutamia tärkeitä asioita. Ensinnäkin tietoa tulee käsitellä oikeudenmukaisesti ja tiedon tulee olla asianmukaista, rajoitettua, mutta kuitenkin tapauksen kannalta riittävää. Henkilötietojen tulee olla ajanmukaisia. Lisäksi tietoja tulee hankkia vain jotain tiettyä tarkoitusta varten, eikä niitä saa pitää hallussa kauempaa kuin tarkoitus vaatii.

Verkko-opiskelussa tärkeimpiä suojattavia tietoja opiskelijoiden näkökulmasta ovat opiskelijoiden henkilötiedot kuten nimi, osoite, puhelinnumero, sähköpostiosoite jne. Opettajan on huomioitava opiskelijan yksityisyyden suojaaminen langattomassa verkko-opiskeluympäristössä. Ilmoittautuessaan kursseille opiskelija luovuttaa omia henkilötietojaan. Lapin yliopistossa käytetään Oodi- tietojärjestelmää, jossa opiskelija ilmoittautuu läsnä- tai poissaolevaksi, ilmoittautuu kursseille sekä pystyy seuraamaan omia opintosuorituksia. Henkilökunta käyttää Oodia opetuksen aikataulutuksekseen, kurssisuoritusten hallinnointiin ja tiedottamisen. Opiskelijan ilmoittauduttua jollekin kurssille hänen henkilötietonsa ovat tällöin kyseisen kurssin opettajan nähtävissä. Opiskelijoiden henkilötietojen käsittelyssä sovelletaan vuonna 1999 säädettyä henkilötietolakia. Esimerkiksi opiskelijan kotiosoite, sähköpostiosoite, puhelinnumero jne. kuuluvat henkilötietoihin, jota ei saa ilman opiskelijan lupaa julkaista verkossa. Myös opiskelijan kurssiarvosanojen julkaisemiseen tarvitaan opiskelijan lupa.

3.3 Langaton verkko

Langaton verkko (WLAN = Wireless Local Area Network) tarkoittaa vähintään kahden koneen keskinäistä kommunikaatiota ilman kaapeleita standardeja verkkoprotokollia käyttäen. Protokolla sisältää tietokoneiden välisen viestinnän säännöt ja kielen, jolla tietokoneet kommunikoivat tietoverkossa. Langattomat verkkolaitteet käyttävät radiotaajuuksia ja niihin liittyvää tiedonsiirtoteknologiaa. IEEE (Institute of Electrical and Electronics Engineers) on määritellyt yleisimmin käytetyn standardin 802.11. Se määrittelee radiotaajuuksilla toimivien langattomien verkkojen ominaisuudet.

Langattoman verkon peittoalue tarkoittaa sitä aluetta, jolla langattoman verkkoyhteyden voi muodostaa työaseman ja tukiaseman välille. Kantama tarkoittaa etäisyyttä, joka muodostuu sisä- ja ulkotiloissa työasemista langattoman verkon tukiasemaan. Kantama voi olla sisätiloissa 50–180 metriä, mutta se voi olla myös pienempi, jos rakenteet vaikuttavat radiolähetyksiin. Ulkotiloissa kantama on noin 300 metriä riippuen sijainnista ja ympäristöstä. Tukiasemat liitetään toisiinsa yleensä lähilankaverkon kautta. Alueella voidaan käyttää useampia tukiasemia, jos se on liian laaja yhdelle tukiasemalle.

Langattomaan lähiverkkoon hakeutuakseen koneessa täytyy olla langaton verkkokortti, joka löydettyään oikean kanavan alkaa keskustella tukiaseman kanssa. Langattoman lähiverkon etuina voidaan pitää edullisuutta, mobiilisuutta, nopeaa ja joustavaa käyttöönottoa, sovelluksien riippumattomuutta sekä suorituskykyä.

Langattomassa verkossa tietoturvariskit ovat samankaltaiset ja yleensä suuremmat kuin lankaverkossa. Langattoman verkon tietoturvassa hyödynnetään WEP- ja WPA-salausmenetelmiä. WEP eli Wireless Encryption Protocol suunniteltiin tarjoamaan langattoman tietoverkon käyttäjille vastaava tietoturva kuin lankaverkoissa. WEP-salausmenetelmä on tietyissä tilanteissa murrettavissa. Tavalliselle käyttäjälle WEPin tarjoama suoja on kuitenkin usein riittävä. Sen rinnalla käytetään usein verkkokorttien MAC-osoitteisiin pohjautuvaa suodatusta. WPA (Wi-Fi Protected Access) -salaus, jota myös Lapin yliopisto käyttää, on kehitetty paikkaamaan WEPin tietoturva-aukkoja. WPA:ta pidetään toistaiseksi murtamattomana.

3.3.1 Lapin yliopiston langattoman verkon tekninen toteutus

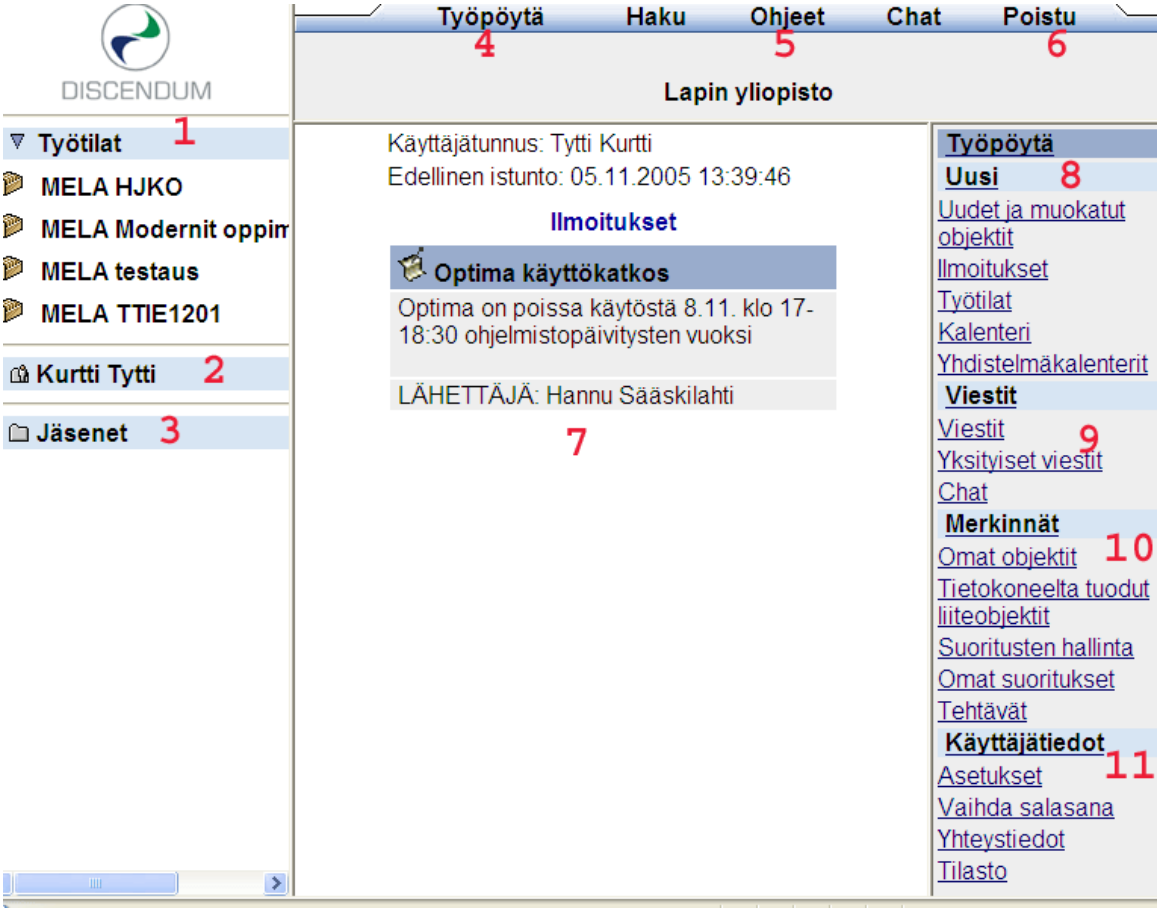
W-Campus on Lapin yliopiston opiskelijoille sekä henkilökunnalle tarkoitettu langaton lähiverkko (WLAN), joka toimii yliopiston sisätiloissa. Verkon käyttämiseen tarvitaan kannettava tietokone tai muu päätelaite sekä yliopiston käyttäjätunnukset. Käyttäjät kirjautuvat langattomaan verkkoon omalla henkilökohtaisella käyttäjätunnuksella sekä verkkotilin salasanalla. Tietokoneesta tulee löytyä langaton verkkosovitin, joka tukee IEEE 802.11b tai IEEE 802.11g -standardia. Lisäksi langattoman verkkosovittimen ajurisovelluksen on tuettava WPA-salausta. Käyttäjän tulee huolehtia omatoimisesti tietokoneensa virustorjunnan sekä palomuuriohjelmistojen ylläpidosta. Opiskelijat saavat lisätietoja opiskelijoiden HelpDeskistä: helpdesk@ulapland.fi. Opettaja voi pyytää neuvoja ja lisätietoja atk-palveluiden neuvonnasta: atkneuvonta@ulapland.fi.

Atk-palvelut on koonnut verkkoon Lapin yliopiston tietoturvaan liittyvää materiaalia, johon jokainen voi käydä tutustumassa (http://www.ulapland.fi/atk). Sivuilta löytyvät muun muassa Lapin yliopiston tietoturvapolitiikka ja –ohjeistus sekä tarkempaa tietoa Lapin yliopiston langattomasta kampuksesta.

3.3.2 Optima verkko-opiskeluympäristö

Lapin yliopisto käyttää Discendum Optima -verkko-opiskeluympäristöä, josta vastaa toistaiseksi opetuksen kehittämispalvelut. Tarkempaa informaatiota Optimasta löytyy Discendumin kotisivulta. (http://www.discendum.com). Sieltä löytyvät muun muassa

Optiman ohjeistus sekä käyttäjän opas. Seuraavaksi esitellään ympäristön keskeisimpiä ominaisuuksia.



Kuva 1. Discendum Optima

Lapin yliopiston Optima -verkko-opiskeluympäristöön kirjaudutaan sivulla: www.ulapland.fi/Optima. Kirjautumisen jälkeen käyttäjälle avautuu Optiman perustila, josta löytyvät seuraavat toiminnot: Optiman yläpalkin valikosta Työpöytä-sanaa (4) klikkaamalla käyttäjä pääsee aina Optiman perustilaan. Työtila-valikosta voidaan valita haluttu kurssi, jolloin käyttäjä saa näkyviinsä kurssin aloitusnäkymän. Optimaa käyttäessä kukaan pysty tekemään mitään peruuttamatonta virhettä, joka tuhoaisi koko kurssimateriaalin. Ohjeet-kohdasta (5) löytyvät Optiman kehittäjien laatimat yleiset käyttöohjeet. Optiman ominaisuuksista käyttäjä voi lukea linkeistä Käyttöohjeet sekä Ohjeita WWW-selainten asetuksista. Työtilan omistajan ohjeet on tarkoitettu lähinnä kurssien opettajille.

Oikeassa yläkulmassa oleva Poistu (6) lopettaa senhetkisen Optiman käyttökerran ja kirjaa käyttäjän ulos. Poistu-linkin avulla käyttäjä poistuu turvallisesti ympäristöstä siten, etteivät muut mahdolliset saman tietokoneen käyttäjät pääse sen jälkeen hänen tietoihinsa käsiksi. Optimaan voi palata jälleen sisään kirjautumalla. Kirjautuessa sisään Optimaan keskelle näyttöä tulee näkyviin opettajien laittamat ilmoitukset (7). Kesken käytön käyttäjä saa ne uudestaan näkyviin joko klikkaamalla Työpöytä-linkkiä ylävalikossa (4) tai oikean reunan valikon Työpöytä (8) ja Ilmoitukset kautta.

Optiman perustilasta löytyvät muut toiminnot, jotka tukevat käyttäjän työskentelyä ympäristötasolla. Työpöytänsä kautta käyttäjä pystyy hallitsemaan keskitetysti ympäristössä olevat viestit, dokumentit, muistiinpanot, kirjanmerkit ja asetukset. Hakukoneen avulla käyttäjä voi löytää helposti viestejä ja dokumentteja. Haku ulottuu myös dokumenttien sisältöihin. Ohje-linkin alta löytyvät ympäristön käyttöön liittyvät ohjeet. Oikean reunan perusvalikon (8-11) käyttäjä saa näkyviin aina joko vasemman reunan valikon Työtilat (1) tai ylävalikon Työpöytä (4)-kohdan kautta. Uusi-valikosta (8) käyttäjä näkee kerralla kaikkien suorittamiensa kurssien uudet tiedostot, ilmoitukset, eri kurssien perustiedot ja kalenterin. Yhdistelmäkalenteri-toimintoa voit käyttää vain käyttäjän suorittaessa samanaikaisesti useampaa verkkokurssia Optimassa. Viestit-valikosta (9) käyttäjä saa näkyviin kerralla kaikkien kurssiesi keskustelualueet, saamansa yksityiset viestit, sekä listan eri kurssien chateista. Chat mahdollistaa reaaliaikaisen keskustelun. Merkinnät-valikosta (10) käyttäjä saa näkyviin hierarkkisen rakenteen, jossa ovat kaikki eri kursseilla tuottamasi tiedostot ja objektit. Jos käyttäjän on esimerkiksi tallentanut vahingossa jonkin tehtävän vastauksen väärään paikkaan, pystyy hän tätä kautta löytämään sen ja katsomaan, missä kansiossa se on. Käyttäjätiedot-valikon (11) kautta käyttäjä saa muokattavaksi omat perustiedot.

Profiilien avulla opettaja pystyy Optima-opiskeluympäristössä määrittelemään tarkasti ja käyttäjäryhmäkohtaisesti, mitkä toiminnot ja työkalut ovat opiskelijoiden käytössä. Profiilien listauksessa pois ruksatut työkalut ja toiminnot eivät näy opiskelijoille, jolloin opettaja pystyy räätälöimään opiskelijoille tarkoituksenmukaiset käyttöliittymät, joista kaikki turhat ominaisuudet on poistettu. Käyttäjien oikeuksia ja työkaluvalikoimaa voidaan myöhemmin tarvittaessa laajentaa.

3.4 Opettajan valmiudet käyttää langatonta verkko-opiskeluympäristöä

Jotta verkko-opetuksessa saavutettaisiin tietoturvallisuuden huomioiva tavoitetila, verkko-opettajan tulisi pyrkiä hallitsemaan verkko-opetukselle asetettuja vaatimuksia, joita ovat:

- teknisen toiminnan ymmärrys
- pedagoginen osaaminen
- toimintakulttuurin muutokseen sopeutuminen

Verkko-opetuksessa opettajan tulee hyödyntää verkon tarjoamat monipuoliset mahdollisuudet opetuksessa. Opettajan tulisi tietää, miten videoneuvotteluja, chat-ryhmiä tai mobiileja päätelaitteita voidaan käyttää verkko-opetuksessa. Verkkoa opetustilanteessa käyttävän opettajan tulee hallita perinteisten opetuksessa tarvittavien taitojen lisäksi seuraavia asioita: aineiston etsiminen verkosta, aineiston tallentaminen verkkoon, sähköpostin käyttö, keskusteluryhmien käyttö ja niiden mahdollisuuksien hyödyntäminen sekä tekijänoikeus- ja tietosuojalainsäädännön asettamien rajoitusten tunteminen toisten tuottaman aineiston ja henkilötietoja sisältävien listojen julkaisemisesta verkossa.

Yliopiston henkilökunnan sekä opiskelijoiden tulee olla itse aktiivisia tietoturvaan liittyvissä asioissa. Tietoturvallinen käyttäytyminen edellyttää tutustumista tietoturvaohjeisiin ja niin opettajien kuin opiskelijan tulee noudattaa yliopiston tietoturvapolitiikkaa. Tietoturvallisuusohjeissa voidaan määritellä tietoturvapolitiikan lisäksi esimerkiksi Internet-politiikka, sähköpostipolitiikka sekä etätyöpolitiikka. Opettaja

on velvollinen pitämään työhuoneensa ovet lukittuina ja tietokoneen suljettuna käytön jälkeen. Tarkemmat opettajan tietoturvaohjeet löytyvät osoitteesta: http://www.ulapland.fi/tietoturva/ ja valikosta *Tietoturvaohjeita henkilökunnalle*. Hallinnollisesta turvallisuudesta vastaa Lapin yliopiston atk-palvelut. Henkilöstöturvallisuus korostuu erityisesti opetushenkilöstön rekrytoinnissa, sillä tällöin opettaja sitoutuu uuteen toimintakulttuuriin ja tekee sopimuksen noudattaakseen yliopiston sääntöjä.

3.5 Opiskelijan näkökulma langattomassa verkko-opiskeluympäristössä

Opiskelijalta vaaditaan verkko-opiskelussa muun muassa seuraavia ominaisuuksia: ajankäytön hallintaa, vastuullisuutta ja itseohjautuvuutta, yhteistyökykyä, verkkovuorovaikutuksen hallintaa sekä tekniikan hallintaa. Tietie (tietojenkäsittelyä tietotekniikan avulla) -projektissa opiskelijoilta kerättyjen kokemusten perusteella voidaan lisäksi todeta, että vaikka verkko-opiskelu vaatii opiskelijalta enemmän kuin tavallinen lähiopetus, se myös antaa enemmän. Opiskelijalla on myös paremmat mahdollisuudet ja vapautta opiskella omaan tahtiin. Lisäksi ryhmätyöskentely tuo uusia näkemyksiä opiskeluun.

Opiskelijalle voidaan antaa tehtäväksi yksilö- ja ryhmäharjoituksia. Verkko-opiskeluympäristössä on mahdollisuus verkkokeskusteluun. Optimassa tämä tapahtuu Chat- tai keskustelu-toimintojen kautta. Tässä opetuskokeilussa opiskelijat käyttivät keskustelu-toimintoa keskustelutehtäviensä toteuttamisessa. Keskustelut dokumentoituivat Optimaan ja ne olivat kaikkien kurssille osallistuvien opiskelijoiden sekä opettajien nähtävissä.

Yliopiston tarjoama kannettava tietokone on opiskelijan vastuulla. Opiskelijan oma toiminta on ratkaiseva tekijä koneen toimivuudessa. Käyttöturvallisuus ja laitteisto- sekä ohjelmistoturvallisuus on tällöin sisällytetty opiskelijan omaan tietoturvakäyttäytymiseen ja -asenteisiin. Opiskelija tekee yliopiston kanssa sopimuksen verkkotunnustensa osalta. Salasanojen osalta käytetään pakollista salasanan vanhenemismenettelyä, jolloin opiskelijan on vaihdettava salasanansa säännöllisesti. Valtiovarainministeriön VAHTI eli valtionhallinnon tietoturvallisuuden johtoryhmä on koostanut myös opiskelijalle sopivan tietoturvaohjeistuksen, joka löytyy osoitteesta: http://www.yliopistojentt.uta.fi/VAHTI-CD/Sivusto/index.htm.

4 Langattoman opiskeluympäristön tietoturva -opetuskokeilu

Langattoman opiskeluympäristön tietoturva -opetuskokeilussa suunniteltiin, toteutettiin ja arvioitiin kurssi SOIT1305 Langattoman opiskeluympäristön tietoturva. Kurssin tavoitteena oli, että opiskelijat ymmärtävät tietoturvan merkityksen mobiiliverkko-opetuksessa ja -opiskelussa sekä oppimisessa. Opiskelijoilla tuli olla kurssin jälkeen hallussaan menetelmiä, joiden avulla he voivat ottaa tietoturvaan liittyvät näkökohdat huomioon. Kurssi toteutettiin monimuoto-opiskeluna, johon kuuluivat neljä lähiopetusluentoa sekä verkko-opiskelu Optima-opiskeluympäristössä. Optimassa olivat kurssin opetusmateriaali, lähdemateriaali, keskustelupalsta, kurssikalenteri sekä kurssin ohjeet. (Kuva 2.)

Kurssin suorittaakseen opiskelijan tuli osallistua luennoille ja perehtyä luentomateriaaliin. Opiskelija osallistui aktiivisesti verkkokeskusteluun luentojen välillä Optima-opiskeluympäristössä. Yhtä luentoa kohden opiskelija kirjoitti vähintään kaksi viestiä. Luentojen jälkeen opiskelija teki käyttöpäiväkirjan. Kurssin arviointi noudatti asteikkoa 1-5/hylätty. Arvioinneissa otettiin huomioon keskusteluihin osallistuminen sekä käyttöpäiväkirjan kirjoittaminen (minimi 3 sivua). Käyttöpäiväkirjan arvioinnissa katsottiin määrän täyttymisen lisäksi myös luennoilla käsiteltyjen aiheiden kattavuutta sekä käyttäjäkokemuksen aitoa kuvausta. Seuraavassa käyttöpäiväkirjan kirjoitusohjeet:

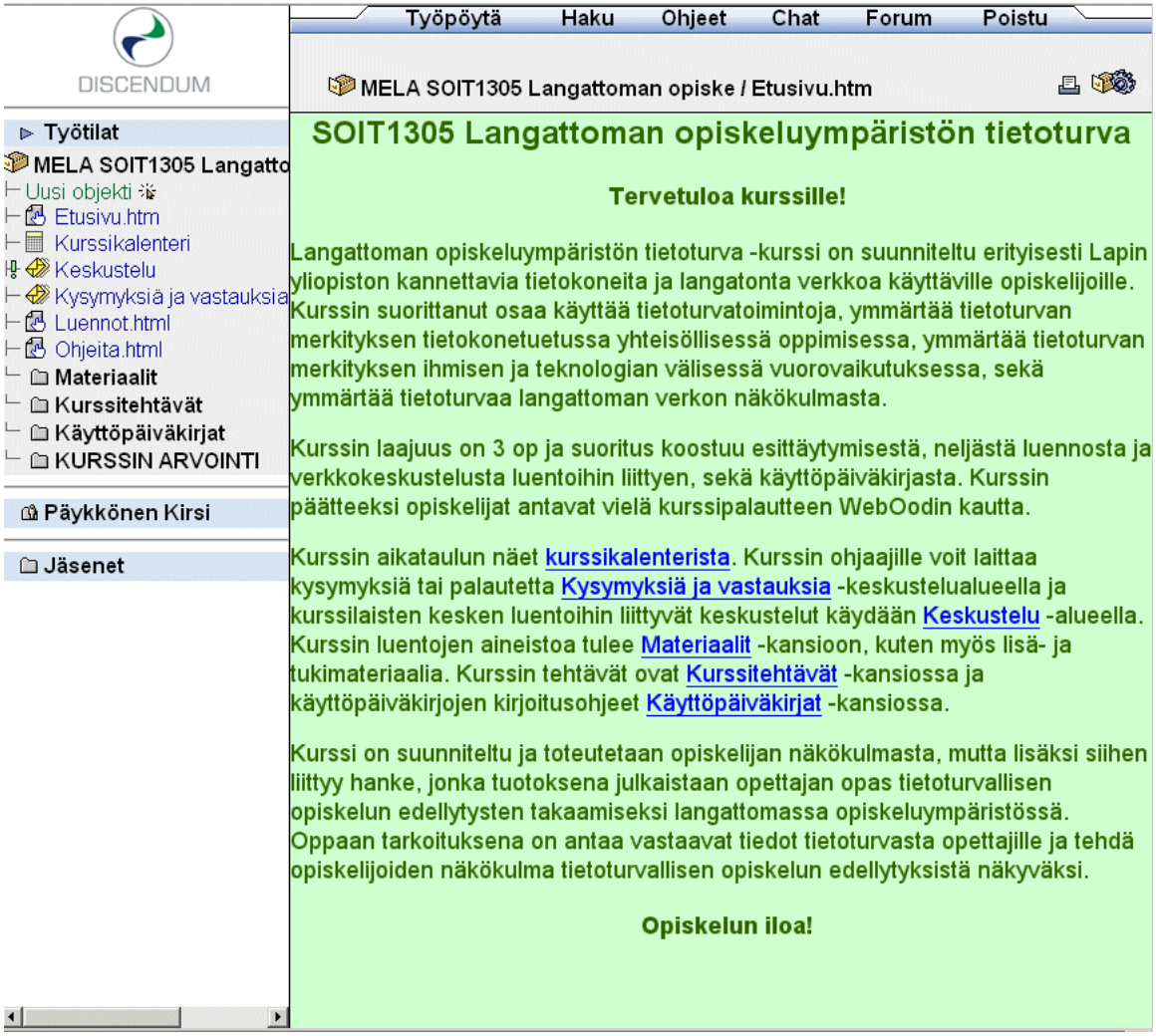
- Käyttöpäiväkirja on luonteeltaan pohdiskeleva kirjoitelma. Sille on ominaista omanäkökulma aiheeseen ja omien arkipäivän käyttökokemusten monipuolinen kuvaaminen. Lähtökohtana on Langattoman opiskeluympäristön tietoturva (SOIT1305) -kurssin luennot ja käydyt keskustelut.
- Kirjoituksessa tulee näkyä kirjoittajan oma näkökulma aiheeseen ja omien kokemusten esittäminen. Pyri kertomaan kokemuksistasi siten, että rakennat vuoropuhelua oman ajattelusi ja kurssilla käsiteltyjen asioiden välille. Tuo rohkeasti esiin oma ajatuksenkulkusi ja oivalluksesi!
- Kiinnitä huomiota kurssin kaikkien osa-alueiden yhdistämiseen (luennot, arkipäivän havainnot, lähdemateriaali ja verkkokeskustelut) kuvailussasi.
- Pohdi tietoturvan merkitystä kannettavien avulla opiskelussasi ja arkielämässäsi, voit mainita myös käyttämiäsi tietoturvaohjelmia (esimerkiksi virustorjuntaohjelmat, palomuurit jne.) ja kertoa, missä tilanteessa ohjelmia käytit.
- Pohdi tietoturvaa myös ihmisen ja teknologian välisen vuorovaikutuksen ja läpinäkyvän käytön kannalta.
- Jos osallistut käyttöpäiväkirjan pitämisen aikana verkkokurssille, kiinnitä huomiota siihen, miten tietoturva-asiat tulevat esiin kurssin aikana.
- Kerro myös langattoman verkon käytöstä, missä tilanteessa sitä käytit ja jos et halua käyttää langatonta verkkoa, voit kertoa myös siitä.

Teknisiä ohjeita

- Rakenne: päiväkirjamainen esitys
- Kirjoitustyyli: kuvailevaa, rikasta tekstiä kannettavien käyttöön ja tietoturvaan liittyen
- Pituus: vapaavalintainen (minimi 3 sivua)
- Kansisivulle : Ylimmäksi kurssin nimi ja päivämäärä. Otsikoksi työn nimi ja sen jälkeen sulkuihin opintosuorituksen koodi ja opintoviikkomäärä. Alle nimesi, opiskelijanumerosi ja yhteystietosi (sposti)
- Fontti : Times New Roman 12 pt.

- Riviväli : 1,5
- Sivunumerointi: alas keskelle

Palautus: 21.11.



Kuva 2. Kurssin perustila Optima -verkko-opiskeluympäristössä.

Kurssi toteutettiin ajalla 3.10.2006–21.11.2006 Lapin yliopiston langattomalla kampuksella. Kurssi sisälsi neljä luentoa, joiden aiheet olivat seuraavat:

1. Tietoturva ja opiskelijan käytännön toimet (Kirsi Päykkönen)
2. Tietokoneella tuetun yhteisöllisen opiskelun tietoturva (Hanna Räisänen)
3. Langattomien verkkojen tietoturva (Kimmo Kokkonen)
4. Tietoturva, oikeusinformatiikka ja käyttöliittymät (Hannakaisa Isomäki).

Seuraavassa kappaleessa kuvataan lyhyesti edellä mainittujen luentojen sisältöä pääpiirteissään.

4.1 Tietoturva ja opiskelijan käytännön toimet

Ensimmäisen luennon tavoitteena oli kertoa opiskelijoille, miten he voivat käytännön toiminnallaan vaikuttaa tietoturvaan käyttäessään kannettavaa tietokonetta yliopiston langattomassa verkossa. Vaikka langattomien verkkojen tietoturvaan liittyy monia teknisiä riskejä, on käyttäjän toiminta kuitenkin suurin yksittäinen tietoturvariskin aiheuttaja – niinpä luennolla kerrottiin ja näytettiin opiskelijakannettavien keskeisimpien tietoturvaominaisuuksien käyttö.

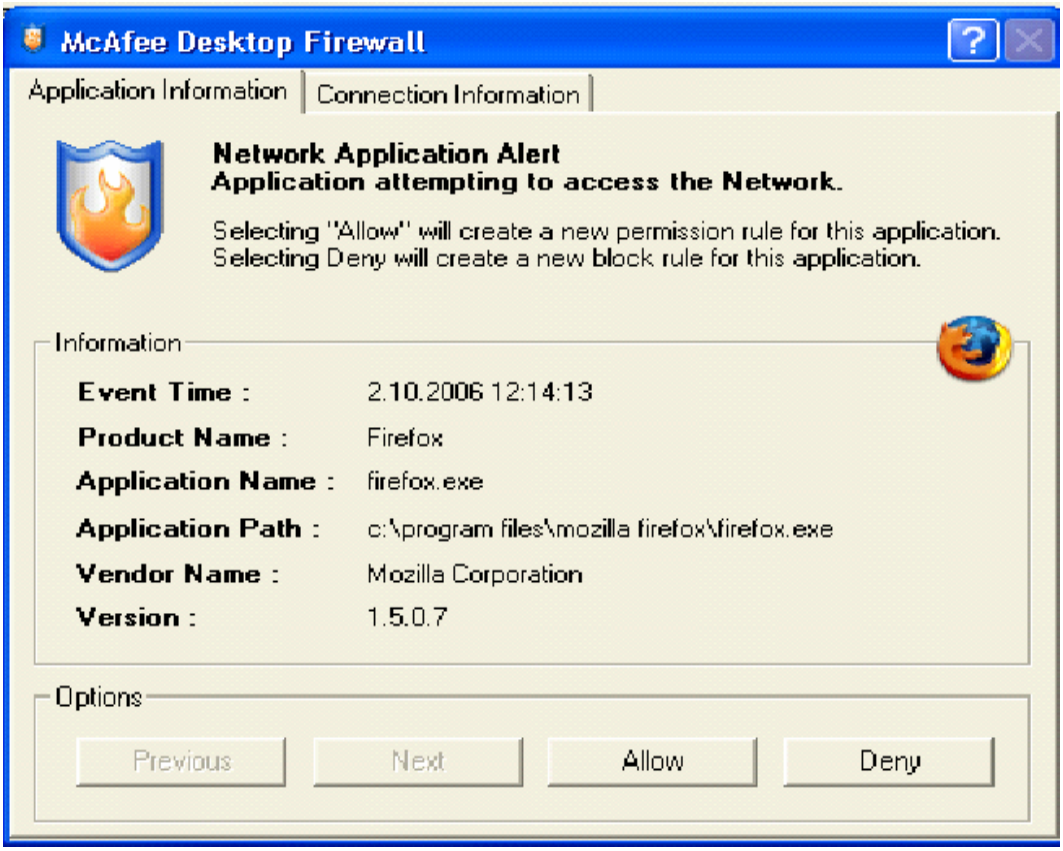
Opiskelijoiden henkilökohtainen tietoturva lähtee niinkin yksinkertaisista asioista kuin kannettavan käsittelystä ja säilyttämisestä – sen huomioimisesta, keillä voi olla tilaisuus päästä tietokoneelle. Koneen sammuttaminen tai verkosta irrottaminen silloin, kun sitä ei käytetä, voi olla järkevä toimenpide, sillä suljettuun tai verkkoyhteydettömään tietokoneeseen ei ainakaan sillä hetkellä voida tunkeutua. Myös tietokoneen suojaaminen salasanoin hankaloittaa koneen luvatonta käyttöönottoa, vaikka se hidastaa myös opiskelijan omaa tietokoneen käyttöä.

Ratkaisevan tärkeä toimi opiskelijan kannettavan tietokoneen käsittelyssä on tietoturvaohjelmien pitämisen ajan tasalla. Palomuurista ja virustutkasta ei juuri ole hyötyä, elleivät ohjelmat ole ajantasaisesti päivitettyjä. Myös käyttöjärjestelmän pitäminen päivitettynä parantaa tietoturvaa, koska päivityksissä on usein paikattu käyttöjärjestelmän tunnettuja tietoturva-aukkoja.

Palomuurilla tarkoitetaan ohjelmaa tai laitetta, joka hallinnoi koneelle tulevaa ja koneelta lähtevää liikennettä. Palomuurin käyttöönoton jälkeen oletusarvoisesti kaikki yhteydet kannattaa olla kiellettyjä, kunnes yksitellen sallitaan haluttujen ohjelmien yhteydet. Windowsin palomuuri ei ole yksin riittävä.

Opiskelijakannettaviin on asennettu McAfeen palomuuri, jota käyttäessään opiskelija voi allow- ja deny-valinnoilla hallita tietokoneensa liikennettä (kuva2.) Jos käyttäjä estää yhteyden vahingossa, eston saa purettua avaamalla palomuuriohjelman ja valitsemalla Firewell Policy -listasta haluttu rivi. Ohjelman symboleista vihreän ympyrän keskellä oleva risti tarkoittaa sallittua yhteyttä ja punaisen ympyrän keskellä oleva viiva estettyä yhteyttä. Kunkin rivin kohdalla valinnan muuttaminen onnistuu seuraavalla tavalla:

- Properties → Firewell rule → Action: Block (estä) tai Permit (salli)



Kuva 3. McAfee-palomuuriohjelman käyttöä.

Virustentorjuntaohjelmien käytössä riittävän tiheä päivittäminen (tai ohjelman automaattisten päivitysten salliminen) on keskeinen toimenpide, jotta ohjelma suojaisi jatkuvasti muuttuvalta haittaohjelmajoukolta. Virustorjuntaohjelmien lisäksi käyttäjän järkevä ja harkitsevainen toiminta on hyvä suoja viruksilta. Esimerkiksi epäilyttäviä tiedostoja ei kannata avata tai ladata koneelle, eikä asentaa epämääräisiä tai epäilyttävistä lähteistä saatuja ohjelmia. Virusilmoituksiinkaan ei kannata luottaa sokeasti, sillä hoaxit eli huijausvaroitukset voivat sähköpostipalvelinten turhan kuormituksen lisäksi saada käyttäjän itse vahingoittamaan tietokonettaan. Hoaxin voi tunnistaa ketjukirjemäisyydestä, ja tarvittaessa virusvaroitusviestin oikeellisuuden voi tarkistaa esimerkiksi Internetin tietoturvaohjelmistoja tarjoavan yrityksen www-sivujen hoax-listasta. Opiskelijakannettavissa virustutkana on McAfeen VirusScan Enterprise.

Mikäli omalla koneella on jo viruksia, ensimmäinen toimenpide on rajoittaa koneen verkkoyhteyksiä viruksen leviämisen estämiseksi. Kun kone on tarkastettu virustorjuntaohjelmalla, on seuraava askel virustutkan päivittäminen ja paikkausten hakeminen Windowsin tietoturva-aukkoihin. Ellei virustorjuntaohjelma pysty poistamaan virusta, käyttäjä voi tarvita erityisiä poistotyökaluja, joita on saatavilla Internetissä. Avun pyytäminen joltain muulta henkilöltä on myös monien käyttämä selviytymiskeino tällaisissa tilanteissa.

Salasanojen suhteen opiskelijan kannattaa muistaa, ettei salasanaksi kannata valita mitään luonnollista sanaa, joka on helposti arvattavissa tai pääteltävissä. Salasanaan kannattaa valita satunnaisia merkkejä ja sen tulee olla riittävän pitkä, esimerkiksi vähintään kahdeksan merkkiä. Salasanoja kannattaa vaihdella säännöllisesti, eikä

samaa salasanaa tule käyttää useassa eri palvelussa tai ohjelmassa. Lisäksi salasanoja ei kannata kuljettaa paperille kirjoitettuna mukana helposti löydettävässä paikassa kannettavan tietokoneen lähellä.

Windowsin käyttäjätilit tarjoavat myös mahdollisuuden parantaa tietoturvallisuutta. Normaalissa käytössä olevalle tilille kannattaa antaa oikeudet vain tarpeellisiin toimintoihin, eli ottaa käyttöön sekä järjestelmänvalvojanoikeuksilla varustettu ylläpitotili että rajoitetumpi tili. Näin rajoitettua tiliä käyttäessään ei tule epähuomiossa asentaneeksi esimerkiksi ohjelmaa, joka tekee muutoksia koko tietokoneeseen.

Eri Internet-selainten tietoturvan taso vaihtelee, esim. Internet Explorer on tietoturvallisuudeltaan heikon selaimen maineessa muihin suosittuihin selaimiin verrattuna. Kuten muidenkin ohjelmien, myös www-selainten päivitykset kannattaa pitää ajan tasalla. Internetissä liikuttaessa harkintaa kannattaa käyttää ActiveX-komponenttien, evästeiden ja Java-sovellusten hyväksymisessä ja sallia ne vain silloin, kun niiden lähde on luotettava ja niiden käyttö on tarpeellista. Omien henkilökohtaisten tietojen yksityisenä pysymiseksi selainhistorian (mm. sivuhistoria, tallennetut lomaketiedot, tallennetut salasanat, latauslista, evästeet, väliaikaistiedostot) tyhjentäminen aika ajoin voi olla hyväksi, etenkin, jos samalle koneelle on pääsy useammalla ihmisellä.

Lapin yliopistolla on käytössä Discendum Optima -verkko-opiskeluympäristö, jossa on eritasoisilla käyttöoikeuksilla varustettuja käyttäjäprofiileja. Opiskelijan on mahdollista eri objektien luku- ja kirjoitusoikeuksien avulla päättää, keillä on pääsy hänen tuottamiinsa dokumentteihin.

Ensimmäisen verkkokeskustelun aiheena oli alkuverryttely ja opiskelijan itsensä esittely. Virikkeenä ensimmäiseen verkkokeskusteluun käytettiin seuraavaa kysymystä: Oletko käyttänyt luennolla esitettyjä tai joitain muita tietoturvaohjelmia? Millaista niitä oli käyttää, kerro hyvistä ja huonoista puolista? Kuinka ilmeistä ohjelmien ja langattoman verkon tietoturvaominaisuuksien käyttö oli käyttöliittymän perusteella, ilman erillisiä ohjeita?

Verkkokeskustelu toteutettiin ajalla 3.10–5.10.2006

4.2 Tietokoneella tuetun yhteisöllisen opiskelun tietoturva

Luennoilla avatut käsitteet:

- CL – Yhteisöllinen opiskelu (Collaborative Learning)
- CSCL – Tietokoneilla tuettu yhteisöllinen opiskelu (Computer Supported Collaborative Learning)
- SCSCL – Tietokoneilla tuetun yhteisöllisen opiskelun tietoturva (Secure Computer Supported Collaborative Learning)

Yhteisöllisen opiskelun keskeinen tunnuspiirre on se, että ajattelun katsotaan olevan erottamaton osa sosiaalista, kulttuurista ja historiallista ympäristöään. (Wertsch 1991, Lave & Wenger 1991) Tutkimuksen kohteena on keskustelu, johon opiskelijat osallistuvat sekä välineet, jotka välittävät oppimista. Yhteisöllinen tiedonrakentelu on

kehämäinen prosessi, jossa yksilöiden ”hiljainen” ymmärrys käsiteltävästä asiasta tehdään näkyväksi (Stahl 2004.)

Tietokoneilla tuetussa yhteisöllisessä opiskelussa opiskelija on osa opiskeluyhteisöä, jonka sosiaalista vuorovaikutusta ja yhteisöllisiä opiskelumenetelmiä tuetaan tieto- ja viestintätekniikalla (TVT). Verkko-opiskelun lisäksi voidaan nykyisin puhua myös mobiiliopiskelusta, millä tarkoitetaan mobiililla teknologialla tuettua opiskelua. Mobiileja laitteita ovat esimerkiksi PDAt (Portable Digital Assistant), kannettavat tietokoneet, kannettavat multimediasoittimet (esimerkiksi Ipod) sekä matkapuhelimet. Mobiilisuus viittaa siis liikuteltaviin laitteisiin, ei opiskeluun tai oppimiseen sinänsä.

Teknologiaa voidaan käyttää opiskelussa usealla tavalla: yhteisöllinen opiskelu voi toteutua esimerkiksi tietokoneen ympärillä tai tietokoneiden ja verkkojen välityksellä. Yhteisöllisen opiskelun perusprosessit ovat samankaltaisia kasvokkain ja verkossa tapahtuvassa opiskelussa, mutta vuorovaikutus on erilaista. Verkkovuorovaikutuksen erityispiirteitä ovat jako samanaikaiseen (synkroninen) ja eriaikaiseen (asynkroninen) vuorovaikutukseen sekä nonverbaalisen viestinnän minimaalisuus. Teknologian suhteuttaminen olemassa oleviin yhteisöllisen opiskelun tapoihin on haasteellista ja joskus hankalaakin, sillä teknologia on usein irrallinen ja riippumaton olemassa olevista käytännöistä ja välineistä. Järjestelmissä on lisäksi toiminnallisia heikkouksia ja virheitä, eikä jokaiseen opetus- ja opiskelutilanteeseen ole olemassa räätälöitävissä olevaa ohjelmaa.

Tieto- ja viestintätekniikkaan pohjautuvien tai niitä hyödyntävien opiskelu- ja oppimisympäristöjen tarkastelussakin keskeisessä asemassa on opiskelu ja sen tavoitteet, ei siis teknologia tai sen ominaisuudet. Tietoturvan rooli on palvella opiskelun tavoitteiden saavuttamista. Tietoturvaa tietokoneilla tuetussa yhteisöllisessä oppimisessa ei juuri ole tutkittu, eli se on uusi tutkimusalue. Tietoturvasta voidaan kuitenkin yleisesti todeta se, että mitä enemmän opiskeluympäristössä käytetään tietoturvaa parantavia toimintoja ja käytänteitä, sitä epämukavampaa toiminnasta tulee ja päinvastoin. Tietoturva edellyttää käyttäjätunnusten ja salasanojen muistamista, niiden vaihtamista, oikeustasojen määrittelyä ja tarkastuksia.

Kuten yleensä tietoturvassa, keskeisiä toiminnan turvallisuuteen vaikuttavia tekijöitä ovat käyttäjät itse. Tämä pätee siis myös tieto- ja viestintätekniikkaa käyttäviin opiskeluympäristöihin. Jos käyttäjät noudattavat tietoturvallisia toimintatapoja, se voi esimerkiksi kasvattaa luottamusta verkko-opiskeluympäristöä kohtaan, mikä edesauttaa yhteisöllisten toimintatapojen toteuttamista.

Toisen luentokerran verkkokeskustelutehtävä oli seuraava: Muodostakaa yhteinen näkemys siitä, mikä on tietoturvan rooli tietokoneilla tuetussa yhteisöllisessä opiskelussa.

Verkkokeskustelu toteutettiin ajalla 5.10–11.10.2006

4.3 Langattomien verkkojen tietoturva

Langattomissa tietoverkoissa esiintyy neljä geneeristä tietoturvapalvelua, jotka ovat luottamuksellisuus, eheys, todennus ja kiistämättömyys. Näistä voidaan johtaa myös pääsynvalvonta sekä saatavuus/käytettävyys. Luottamuksellisuus tarkoittaa sitä, että tiedot ja järjestelmät ovat vain niiden saatavilla, joilla on niiden käyttöön oikeutus. Tietoja ei myöskään paljasteta sivullisille. Luottamuksellisuus tarkoittaa myös tietojen suojaamista luvatonta käyttöä vastaan. Eheys tarkoittaa, että tietoa voivat muuttaa vain ne käyttäjät, joilla on siihen oikeutus. Eheys säilyy, kun tiedot ja järjestelmät ovat luotettavia, oikeellisia ja ajantasaisia. Eheydellä pyritään tiedon ja sen käsittelytapojen täydellisyyteen ja virheettömyyteen.

Todennus eli autentikointi varmistaa sen, että käyttäjä on se, kuka hän väittää olevansa. Todennus tarkoittaa osapuolten (henkilö, järjestelmä tai järjestelmän osa) luotettavaa tunnistamista. Kiistämättömyys tarkoittaa sitä, että käyttäjän tekemät muutokset voidaan jäljittää. Tavoitteena on tällöin pystyä todistamaan tapahtunut jälkeenpäin. Kiistämättömyys on tärkeää erityisesti sähköisessä asioinnissa. Pääsynvalvonta käsittää ne toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille. Saatavuus/käytettävyys tarkoittaa sitä, että järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä tietyn vasteajan puitteissa. Saatavuudella varmistetaan tietojen tuhoutumattomuus sekä tietojärjestelmien toiminnan turvaaminen. Saatavuus/käytettävyys varmistaa myös jatkuvuuden turvaamisen poikkeavissa olosuhteissa.

Tietoturvaan kohdistuvissa hyökkäyksissä ja uhkissa käytetään luokittelua teknisiin menetelmiin ja sosiaaliseen hakkerointiin. Tekniset menetelmät sisältävät aktiiviset ja passiiviset hyökkäykset. Lisäksi hyökkäyksiä voidaan luokitella myös kohteen mukaan eli palvelimeen, verkkoon tai sen osaan kohdistuviin hyökkäyksiin. Sosiaalinen hakkerointi (Social Engineering) kattaa tekniikat, joilla pyritään manipuloimaan käyttäjiä suorittamaan toimintoja tai luovuttamaan luottamuksellisia tietoja. Tavoitteena on tällöin joko esiintyä toisena käyttäjänä tai kerätä tietoa. Passiiviset hyökkäykset muodostuvat liikenteen salakuuntelusta (Passive Eavesdropping) ja liikenteen monitoroinnista (Traffic Analysis). Tavoitteena on tällöin kerätä dataa, ei muuttaa sitä. Passiivisia hyökkäyksiä on vaikea havaita, mutta niiltä voidaan suojautua liikenteen salauksella. Aktiiviset hyökkäykset sisältävät joko siirrettävän tiedon muuttamista, virheellisen tiedon syöttämistä järjestelmään tai näiden yhdistelmiä. Hyökkäykset voidaan jakaa neljään ryhmään:

1. naamiointi (Masquerade)
2. toisto (Replay)
3. viestin muuttaminen (Modification)
4. palvelunesto DOS (Denial-Of-Service).

Langattomia verkkoja ei voida rajata fyysisesti tietylle alueelle. Tiedon kerääminen passiivisin menetelmin on helpompaa kuin langallisissa verkoissa. Langattomissa verkoissa verkon tukkiminen ja palvelunestohyökkäyksen tekeminen on helpompaa kuin langallisissa verkoissa. Hyökkäyksiä on myös vaikeampi havaita, jäljittää ja estää. Langattomissa verkoissa hyökkäyksen toteuttamiseksi ei tarvita järjestelmässä sisällä olevia laitteita tai resursseja. Hyökkäyksissä voidaan käyttää ilmaisia, Internetissä vapaasti saatavilla olevia ohjelmia. Yleisimpänä ongelmana ovat huonosti konfiguroidut verkon komponentit.

Yleisimmin käytetty salausmenetelmä langattomissa verkoissa on WEP (Wired Equivalent Privacy), mikä on kehitetty tarjoamaan turvallinen tiedonsiirto päätelaitteen ja tukiaseman välille. WEP on suunniteltu tarjoamaan sama turvallisuuden taso, joka on saavutettu langallisissa verkoissa. WEPin tavoitteena on toteuttaa pääsynvalvontaa (Access Control) sekä taata luottamuksellisuus salaamalla viestit WEP-avaimen avulla. WPA (Wi-Fi Protected Access) on kehitetty ratkaisuksi WEP-salauksen heikkouksiin. WPA koostuu neljästä uudesta algoritmista, jotka liittyvät: salauksen parantamiseen, eheyden tarkistamiseen, todentamiseen sekä avainten hallintaan. Lisäksi on olemassa EAP (Extensible Authentication Protocol) ja 802.11x, jotka tarjoavat eri menetelmiä käyttäjän todentamiseksi.

Langaton ympäristö avaa hyökkääjälle uusia mahdollisuuksia ja aiheuttaa pieniä muutoksia hyökkäysmenetelmiin. Langaton verkko voi toimia takaporttina langalliseen verkkoon. Hyökkäykset tapahtuvat kolmea verkon perusominaisuutta vastaan. Luottamuksellisuutta vastaan hyökätessä kaapataan tietoja, selvitetään tunnistetietoja ja salasanoja. Eheyttä vastaan hyökätään muuttamalla tietoa tai laitteiden asetuksia. Käytettävyyttä vastaan hyökätään palvelunestohyökkäyksillä. Verkon löytäminen on yleisin hyökkäys langattomia lähiverkkoja vastaan. Hyökkäykset ovat helposti järjestettävissä vähäisten laitevaatimusten sekä tarvittavien ohjelmien vapaan saatavuuden vuoksi. Luvattoman päätelaitteen kytkemisessä verkkoon (Rogue Adapter) tavoitteena on ilmaisen Internet-yhteyden hyödyntäminen ja luottamuksellisen tiedon etsiminen verkon sisältä. Salakuuntelulla tarkoitetaan verkossa kulkevan tiedon kaappaamista. Tiedot ovat yleensä tunnistetietoja, verkkoinformaatiota sekä muuta kiinnostavaa informaatiota. Salakuuntelu on usein osana muita hyökkäyksiä ja useat hyökkäykset tarvitsevat kaapattua tietoa toteutukseensa. WEP-salauksen käyttämisellä voidaan suojautua salakuuntelua vastaan salaamalla siirrettävä liikenne, mutta salakuuntelun estäminen teknisin menetelmin on vaikeaa. WEP-salauksen heikkous perustuu RC4 algoritmin heikkoon alustusvektoriin. WEP-salauksen purkuun on vapaasti saatavilla olevia purkuohjelmia.

Luvaton tukiasema (Rogue Access Point) tarkoittaa kahta asiaa: luvallisen käyttäjän luvatonta tukiasemaa, joka voi huonosti asennettuna muodostaa aukon verkon turvallisuuteen tai vihamielisen käyttäjän luvattomasti rakennettua tukiasemaa. Niillä on yleensä kaksi käyttötarkoitusta: palvelunestohyökkäys asettamalla oma tukiasema vahvalla signaalilla tai oikeana verkkona esiintymistä ja verkkoliikenteen kaappaamista (Man-In-the-Middle). Uusimmat menetelmät kohdistuvat tukiasemien ohjelmistojen heikkouksien etsimiseen sekä langattomien verkkokorttien ajureiden heikkouksien etsimiseen.

Kolmas verkkokeskustelutehtävä oli seuraava: Käykää Optimassa keskustelua siitä, millainen käsitys teille jäi langattomien verkkojen tietoturvatasosta? Pohtikaa myös samalla sitä, millaisia ongelmia/riskejä langattomuus tuo oppimisympäristöjen turvalliselle käyttämiselle?

Verkkokeskustelu toteutettiin ajalla 11.10–17.10.2006

4.4 Tietoturva, oikeusinformatiikka ja käyttöliittymät

Luvussa on käytetty seuraavia lähteitä:
Isomäki, H. 2004. Toteutuuko käyttäjien oikeusturva sähköisissä palveluissa? [Does Users' Legal Protection Come True in Electronic Services?]. Tietosuoja/Dataskydd 3, 28–31.
Isomäki, H. & Hof, S. 2005. On Information, Law and User Interfaces of e-Government Services. In Viborg Andersen, K., Grönlund, Å., Traunmüller, R. & Wimmer, M. (Eds.) Electronic Government – Workshop and Poster Proceedings of the Fourth Internaational EGOV Conference 2005, August 22-26, Copehagen, Denmark. Linz, Austria: Schriftenreihe Informatik 13 Universitätsverlag Rudolf Trauner, 398-408.

Sähköisten koulutuspalvelujen käyttöliittymien tulisi olla sellaisia, että käyttäjien informaatioon ja viestintään liittyvät perusoikeudet toteutuvat. Oleellista on liittymien helppo käytettävyys. Langattomat verkko-opiskeluympäristöt ja niiden avulla toteutettava sähköinen viestintä ja koulutuspalvelut asettavat erityisvaatimuksia käyttöliittymille.

4.4.1 Toteutuuko käyttäjien oikeusturva sähköisissä palveluissa?

Sähköisten palveluiden rakentaminen yksityisen sektorin ja julkishallinnon palvelujärjestelmiin on tyypillistä nykyiselle tietoyhteiskunnalle. Organisaatioissa kehitetään ja hajautetaan yhä enemmän asiakastoimintoja informaatioteknologiaan perustuen. Sähköisten palveluiden kehittäminen näissä uudentyyppisissä palvelujärjestelmissä sisällyttää sekä asiakkaat että palvelutuotannon ammattilaiset informaatioteknologiaa hyödyntäviin toimintamalleihin siinä määrin, että kehittämistyön perusoletuksena selvästikin pidetään sähköisten palveluiden integroitumista osaksi ihmisten arkea. Se, hyväksyvätkö käyttäjät uudet sähköiset palvelujärjestelmät osaksi elämäntapaansa, riippuu paljon järjestelmien käyttöliittymien ominaisuuksista.
Käyttöliittymät tarjoavat käyttäjilleen tiedollisen, kielellisen ja toiminnallisen yhteyden informaatioteknologialla toteutettuun palvelujärjestelmään. Käyttöliittymät ovat yleensä graafisia ja koostuvat useista komponenteista, joista tärkeimpiä ovat ikkunat, valikot ja kuvakkeet.

Keskeistä käyttöliittymän toteuttamisessa on, että se on vuorovaikutteinen: käyttöliittymän tarkoitus on sekä antaa käyttäjälle informaatiota että ottaa tältä vastaan informaatiota riittävästi ja oikealla tavalla. Toimintojen tulee olla yksinkertaisia ja luonnollisia käyttää ja – kuten suomalainen ja EU-lainsäädäntö erityisesti sähköisestä asioinnista määrittelee – käytettäviä. Lisäksi käyttöliittymien ominaisuuksien tulisi osaltaan turvata käyttäjien perustavanlaatuisia informaatioon ja viestintään liittyviä oikeuksia. Tietoyhteiskunnan vaatimukset sähköisten palvelujärjestelmien käyttöliittymille voidaan siis määritellä kahden moniulotteisen käsitteen avulla: käyttöliittymien tulee olla sekä käytettävyyden eri kriteerien että käyttäjien informaatio-oikeudellisten perusoikeuksien kanssa yhdenmukaisia.

4.4.2 Käytettävyys, osa järjestelmän laatua

Käytettävyys on teknologisen tuotteen laatuominaisuus, jolla kuvataan, kuinka helppoa, miellyttävää ja tehokasta tuotetta on käyttää. ISO 9241-11 -standardin mukaan

käytettävyys mittaa tuotteen käytön tuottavuutta, tehokkuutta ja miellyttävyyttä. Tuottavuus tarkoittaa sitä, että tehtävät voidaan tehdä täydellisesti ja virheettömästi. Tehokkuus edellyttää järjestelmältä riittävän nopeaa tiedonsiirto- ja tietojenkäsittelykykyä.

Miellyttävyys on käyttäjän subjektiivinen miellyttävyyden kokemus. Miellyttävyys täsmentyy erityyppisiksi, usein tunnepohjaisiksi käyttökokemuksiksi järjestelmän käyttökontekstin mukaan. Sähköisessä asioinnissa tärkein miellyttävyyttä edistävä tekijä on luottamus. Käytettävyydeltään hyvät järjestelmät herättävät luottamusta sekä palvelujärjestelmää että sen tuottajaa kohtaan. Luottamus järjestelmää kohtaan syntyy, kun käyttäjä kokee järjestelmän tekevän oikeita asioita, toimivan varmasti sekä olevan tietoturvaltaan ja tietosuojaltaan hyvää tasoa.

Käytettävyyden keskeisiä kriteerejä sähköisissä palveluissa ovat siten tietoturva, tietosuoja sekä näiden aikaansaama luottamuksen kokemus. Koska järjestelmän ja käyttäjän vuorovaikutusta säätelee käyttöliittymä, on erittäin tärkeätä sisällyttää sähköisen palvelun järjestelmiin sellaisia käyttöliittymiä, jotka sisältävät luottamusta herättäviä ominaisuuksia.

Käyttöliittymätutkimus on tuottanut useita ns. heuristiikkoja käytettävyydeltään hyvien käyttöliittymien suunnitteluun. Keskeisin yksittäinen kriteeristö kuvaa tietoturvallisen käyttöliittymän suunnittelun periaatteita. Tietoturvaan liittyvät periaatteet korostavat luottamusta herättävän käyttöliittymän toteuttamista. Kriteeristö koostuu kuudesta suunnitteluperiaatteesta:

1. Tietoturvaominaisuuksien välittäminen käyttäjälle. Käyttöliittymän tulee välittää käytettävissä olevat tietoturvapiirteet käyttäjälle.
2. Järjestelmän tietoturvatilan läpinäkyvyys. Periaate edellyttää, että käyttäjä voi havainnoida käyttöliittymästä järjestelmän toimintojen eli sen sisältämien sisällöllisten prosessien tietoturvatilaa.
3. Opittavuus. Käyttöliittymän komponenttien merkitys sekä niiden käytön tulee olla helposti opittavissa ja muistettavissa.
4. Esteettinen ja minimalistinen design. Periaatteen mukaan vain relevantti (tietoturva)tieto tulisi näyttää käyttöliittymässä.
5. Virheiden käsittely. Virheilmoitusten tulisi olla yksityiskohtaisia ja ajantasaisia.
6. Tyytyväisyys ja luottamus. Tyytyväisyyden ja luottamuksen kriteeri perustuu edellä esitettyjen kriteerien onnistuneeseen toteutukseen.

4.4.3 Takaavatko kriteerit käyttäjien informaatioon liittyvät perusoikeudet?

Sähköisten palveluiden käyttöönotto, verkkoviestinnän monipuolistuminen ja elektronisen hallinnon yleistyminen ovat johtaneet tilanteeseen, jossa kansalaisten informaatio-oikeudellisten perusoikeuksien käyttö yhdistyy yhä enemmän tietojärjestelmien käyttöön. Käyttöliittymien toteuttamisessa tulee kiinnittää huomiota näiden oikeuksien toteutumismahdollisuuksiin. Keskeisimpiä näistä perustavanlaatuisista oikeuksista ovat oikeus tietoon, oikeus viestintään, oikeus vapaaseen tietoon ja tiedonkulkuun, oikeus tietoturvaan ja tietosuojaan, oikeus tiedolliseen itsemääräämiseen ja oikeus yksityisyyteen. Viestinnällisestä näkökulmasta olennainen periaate on myös oikeus luottamukselliseen viestintään. Onko edellä esitetyillä käytettävyyden periaatteilla yhteyttä käyttäjän oikeudellisia perusoikeuksia

turvaaviin periaatteisiin? Ensimmäinen periaate, jonka mukaan käyttöliittymän tulee välittää käytettävissä olevat tietoturvaominaisuudet käyttäjälle, on yhdenmukainen niiden oikeudellisten periaatteiden kanssa, jotka pyrkivät turvaamaan käyttäjien oikeuksia saada tietoa. Mikäli tietoturva toimii teknisesti hyvin, myös oikeus tietoturvaan ja tietosuojaan todennäköisesti toteutuu ja siten myös oikeus luottamukselliseen viestintään.

Sen sijaan periaate ei selkeästi tue näkemystä, jonka mukaan käyttäjän on voitava myös käyttää tietoa – sen lisäksi, että hänellä on oikeus saada sitä. Tietoturvapiirteiden välittäminen käyttäjälle tulisi toteuttaa käyttöliittymissä siten, että käyttäjä voi näitä piirteitä myös käyttää. Mikäli näin ei ole, käyttäjien oikeus tiedolliseen itsemääräämiseen vaarantuu. Sähköisiä palveluita käytettäessä käyttöliittymän tulee antaa käyttäjille mahdollisuus säädellä prosessoinnin kohteena olevan tiedon suojaamista ja siten yksityisyyden suojaansa.

Oikeus luottamukselliseen viestintään voidaan kyseenalaistaa myös tietokonevälitteisen toiminnan näkökulmasta: käyttäjällä tulee olla oikeus viestiä sen järjestelmän tietoturvapiirteiden kanssa, joka välittää hänen viestejään kolmannelle osapuolelle.

Edellisenkaltainen pulma sisältyy myös toiseen suunnitteluperiaatteeseen. Järjestelmän tietoturvatilan läpinäkyvyyden periaate edellyttää käyttöliittymältä, että käyttäjä voi havainnoida järjestelmän toimintojen tietoturvatilaa. Pelkkä havainnointi ei kuitenkaan anna käyttäjälle välineitä tietoturvatilan säätelyyn. Oikeus saada tietoa todennäköisesti toteutuu, mutta tiedollinen itsemääräämisoikeus sekä oikeus luottamukselliseen viestintään kyseenalaistuvat. Palvelujärjestelmien tietoturvapiirteiden vuorovaikutteisuuden suunnittelun ja toteuttamisen kannalta huomionarvoista on, että luottamuksellisen viestinnän suoja ulottuu viestin sisällön lisäksi viestinnän tunnistamistietoihin. Käyttöliittymille asetettu opittavuuden ominaisuus on osittain yhdenmukainen tietojärjestelmille asetetun käytettävyyden vaatimuksen kanssa. Opittavuus on tärkeä mutta ei ainoa käytettävyyden osa. Opittavuus tukee käyttäjien perustavanlaatuista oikeutta saada tietoa: voidaan katsoa, että tieto on käyttäjällä vasta kun se on havaittu, ymmärretty ja muistettu. Yksinomaan tämä ominaisuus ei kuitenkaan riitä herättämään käyttäjissä luottamusta.

Esteettinen ja minimalistinen design -periaate korostaa, että vain relevantti (tietoturva)tieto tulisi näyttää käyttöliittymässä. Periaate on ongelmallinen, koska siitä ei ilmene, kuka päättää, mikä on relevanttia tietoa. Onko riittävää, että tietojärjestelmän suunnittelija määrittelee, mitä toimintoja käyttäjälle tulee esittää? Tulisiko kysyä käyttäjiltä? Onko riittävää, että edellisten lisäksi käytettävyysasiantuntija määrittelee, mikä on ihmisen havaitsemisen, ymmärtämisen ja muistamisen näkökulmasta tarkoituksenmukaista tietoa? Mikäli halutaan toimia käyttäjien informaatio-oikeudellisia perusoikeuksia turvaten, relevantin tiedon määrittelyyn olisi syytä ottaa mukaan myös tietosuojan asiantuntijoita.

Luottamuksen kannalta kriittisin suunnitteluperiaate painottaa virheilmoitusten yksityiskohtaisuutta ja ajantasaisuutta. Periaate viittaa yksisuuntaiseen vuorovaikutukseen eikä määrittele käyttäjien mahdollisuuksia toimia virhetilanteessa. Tiedollisen itsemääräämisoikeuden kanssa samansuuntaisia suosituksia ei anneta.

Viimeinen suunnitteluperiaate, tyytyväisyys ja luottamus, perustuu edellisten kriteerien onnistuneeseen toteutukseen. Mikäli tässä ei ole onnistuttu, käyttäjien oikeus

tietoturvaan, tietosuojaan, käytettäviin järjestelmiin ja luottamukselliseen viestintään ei toteudu.

4.4.4 Miten käyttäjien oikeudet varmistetaan?

Nykyisten käyttöliittymän suunnittelun periaatteiden valossa näyttää siltä, että käyttöliittymien ominaisuudet eivät turvaa riittävästi käyttäjien informaatioon ja viestintään liittyviä oikeuksia. Tietoyhteiskunnan vaatimukset käyttöliittymille eivät saa riittävää huomiota käytettävyyden eivätkä käyttäjien perusoikeuksien näkökulmista. Siten on todennäköistä, että käyttäjien informaatio-oikeudelliset perusoikeudet eivät toteudu sähköisissä palveluissa. On tarpeen kouluttaa ammattilaisia, jotka hallitsevat käytettävyyden, informaatioteknologian ja oikeusinformatiikan sisältöjä.

Oikeusinformatiikka kuuluu lakimiesten lisäksi erilaisissa tietotehtävissä toimivien välttämättömään osaamiseen. Oikeusinformatiikan tuntemus on tarpeen paitsi tietojärjestelmien suunnittelussa myös aktiivista elektronisen informaation hyödyntämistä vaativissa työtehtävissä, kuten sähköisten hyvinvointipalveluiden kehittämiseen liittyvissä tehtävissä. Tarpeellisia ovat myös ihmiskeskeisten tietojärjestelmien kehittämisen taidot. Käyttäjän kannalta ratkaisevia ovat ”älykkään” tuotteen suunnittelu ja muotoilu, joiden lähtökohtia ovat käytettävyys, sosiaalinen hyväksyttävyys ja jopa elämyksellisyys.

Taulukko 1. Käyttäjien oikeudet

Kriteeri	Kuvaus	Yhteys käyttäjien perusoikeuksiin
1. Tietoturvaominaisuuksien välittäminen käyttäjälle	Käyttöliittymän tulee välittää käytettävissä olevat tietoturvapiirteet käyttäjälle	• oikeus saada tietoa • oikeus tietoturvaan • tiedollinen itsemääräämisoikeus?
2. Järjestelmän tietoturvatilan läpinäkyvyys	Käyttäjän tulisi voida havainnoida järjestelmän toimintojen tietoturvatilaa	• vapaa tiedon kulku • tiedollinen itsemääräämisoikeus? • oikeus luottamukselliseen viestintään?
3. Opittavuus	Käyttöliittymän tulee olla helposti opittavissa	• oikeus käytettäviin järjestelmiin • käytettävyys kokonaisvaltaisesti?
4. Esteettinen ja minimalistinen design	Vain relevantti tietoturvatieto tulisi näyttää	• kuka määrittelee, mikä on relevanttia tietoa?
5. Virheiden käsittely	Virheilmoitusten tulisi olla yksityiskohtaisia ja ajantasaisia	• tiedollinen itsemääräämisoikeus? • oikeus luottamukselliseen viestintään?
6. Tyytyväisyys ja luottamus	Käyttöliittymän tulisi herättää luottamusta käyttäjissä	• oikeus tietoturvaan? • oikeus luottamukselliseen viestintään? • oikeus käytettäviin järjestelmiin?

Neljäs verkkokeskustelutehtävä oli seuraava: Keskustelkaa siitä, miten käyttämänne ympäristön käyttöliittymän tietoturvaan liittyvät kriteerit toteutuvat. Kriteerithän olivat:

1. käyttöliittymä välittää käyttäjälle tiedon käytettävissä olevista tietoturvatoiminnoista – onko näin?
2. käyttöliittymä on ’läpinäkyvä’ suhteessa tietoturvatoimintoihin: käyttäjän on mahdollista käytön aikana havaita järjestelmän tietoturvan tila – onko näin?
3. opittavuus: tietoturvaominaisuuksia on helppo oppia käyttämään – onko näin?
4. tietoturvapiirteiden esteettinen ja minimalistinen design – vain relevantti tieto esitetään: onko näin?
5. virheilmoitukset ovat ajantasaisia ja selkeitä; osaat niiden perusteella korjata tilanteen – onko näin?

6. luottamus ja tyytyväisyys; koetko luottamusta järjestelmän turvallisuutta kohtaan? Mihin ominaisuuksiin luotat ja mihin et? Miksi?

Pohtikaa myös samalla sitä, millaisia puutteita tai etuja edellisestä voi seurata käyttäjän perusoikeuksien toteutumisen kannalta. Perusoikeuksiahan olivat: oikeus tietoon, oikeus (luottamukselliseen) viestintään, oikeus vapaaseen tiedonkulkuun, oikeus tietoturvaan ja tietosuojaan, oikeus tiedolliseen itsemääräämiseen ja oikeus yksityisyyteen. Yksi esimerkki näiden oikeuksien toteutumisen pohtimisesta on Luentomateriaalit -kansiossa, tiedostossa SOIT1305_Isomäki.pdf (sivut 30–32). Tätä pohdintaa voi myös jatkaa käyttöpäiväkirjassa. Pohdi aiheita vapaasti omin sanoin. Osallistu tehtävään vähintään viidellä viestillä kurssin keskustelualueella.

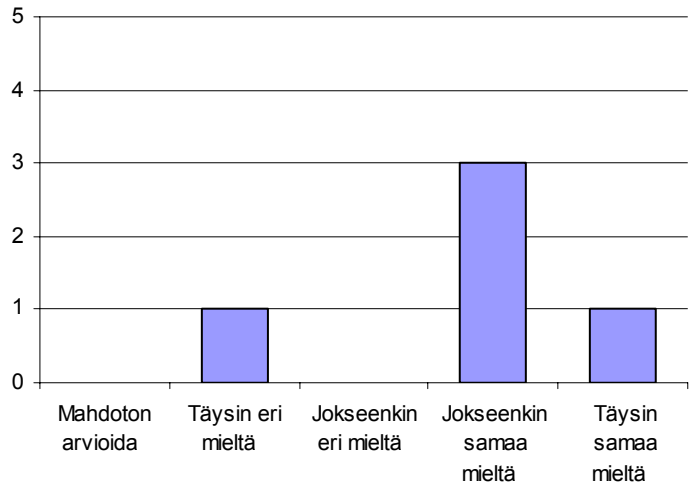
Verkkokeskustelu toteutettiin ajalla 17.10–27.10.2006. Viestien määrää kasvatettiin luennoille osallistuvien vähäisen määrän vuoksi.

5 Opiskelijoiden kokemukset opetuskokeilusta

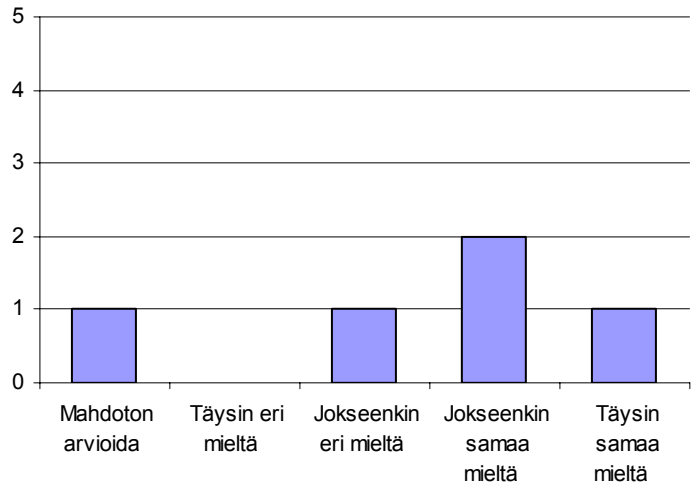
Raportin loppuun on koottu opetuskokeilun toteutumisen arviointi opiskelijoiden näkökulmasta. Seuraavissa kappaleissa on esitetty opiskelijoiden kokemukset kurssista käyttöpäiväkirjoista saatujen tietojen perusteella sekä kurssin opiskelijapalaute.

5.1 Kurssipalaute

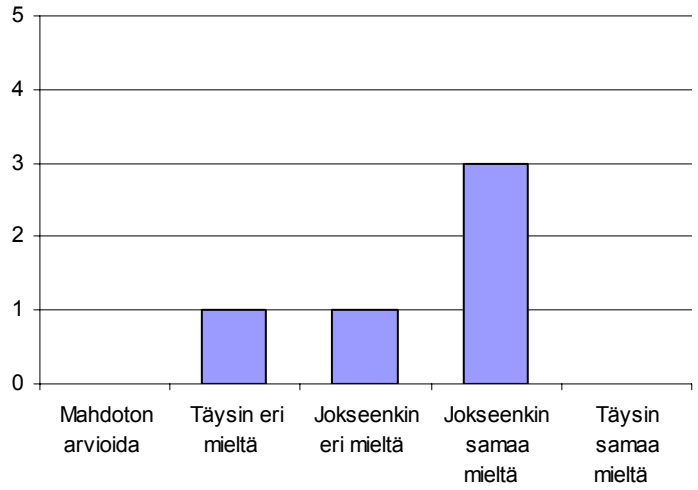
Opiskelijat antoivat kurssipalautteen WebOodin kautta. Alla on palaute esitettynä pylväsdiagrammien muodossa. Palautteessa opiskelijat arvioivat kurssin opetustapaa, kurssin työmäärää, omaa ymmärrystä ja kiinnostusta kurssilla esitettyihin asioihin sekä lähiopetuksen, verkko-opiskelun ja itsenäisen opiskelun määrää.



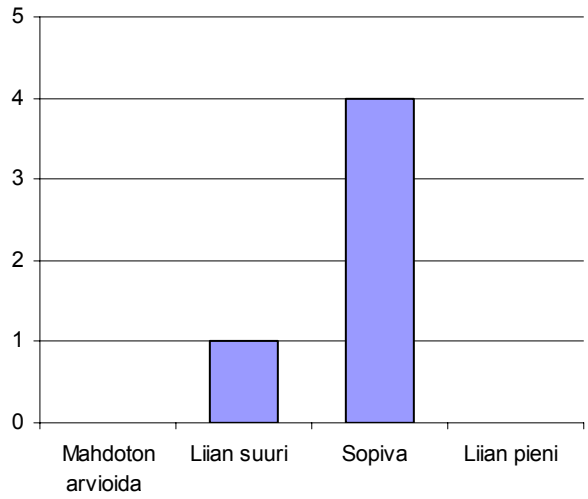
Kuvio 1. Opetustapa soveltui hyvin opintojaksolle määriteltyihin tavoitteisiin



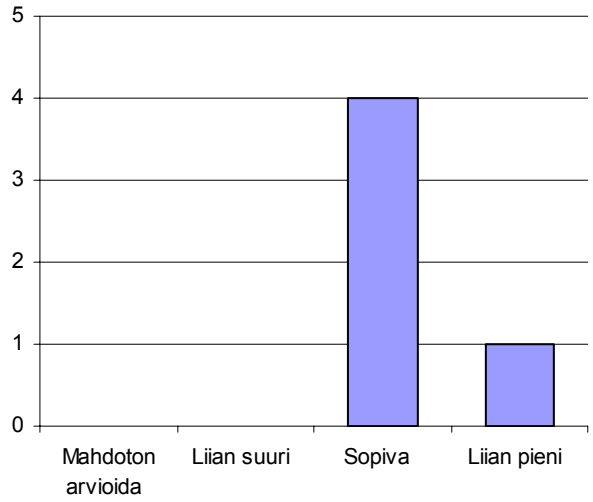
Kuvio 2. Ymmärsin opiskeltavat asiat hyvin.



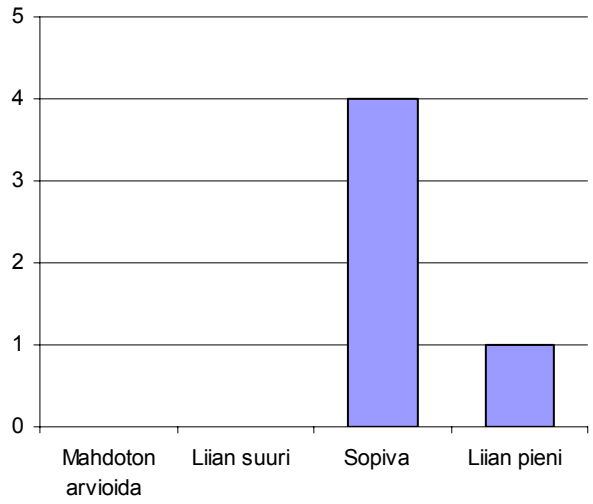
Kuvio 3. Kurssi lisäsi kiinnostustani opiskeltavaan asiaan.



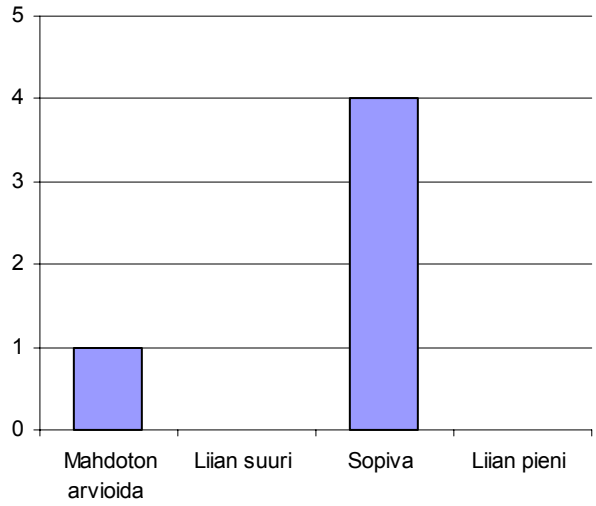
Kuvio 4. Lähiopetuksen määrä.



Kuvio 5. Verkko-opetuksen määrä



Kuvio 6. Itsenäisen opiskelun määrä.



Kuvio 7. Opintojakson työmäärä suhteessa sen tuottamiin opintopisteisiin.

Opiskelijoilla oli mahdollisuus kommentoida omia kokemuksiaan kurssista seuraavien kysymysten avulla:

Mitkä seikat auttoivat opiskeltavien asioiden oppimista?

- *”Se oli hyvä. että kerrankin sai kriittisesti kommentoida asioita ja tuoda omia näkemyksiä esille.”*
- *”Hyvät luentomuistiinpanot ja ohjeistukset.”*

Mitkä seikat haittaisivat opiskeltavien asioiden oppimista?

- *”Ehkä se, että ei saanut käytännössä toteuttaa ja ei niitä suojauksia tehty ja katsottu yhdessä. Toisaalta taas verkkokeskustelu, kun Optima-ympäristö on niin huono. ”*

Miten kurssia voitaisiin kehittää edelleen?

- *”Itse jäin kaipaamaan enemmän sitä käytäntöä. että oltaisiin kunnolla käyty läpi koulun kannettavissa olevat tietoturvaohjelmat kun ne nyt vain pintaseltaan raapaistiin.”*
- *”Kurssikuvauksessa olisi pitänyt lukea vaatimus läsnäolosta luennoilla sekä workshop-töistä. Nyt kuvaus ja kurssin sisältö eivät vastanneet toisiaan. Siksi kurssia ei pystynyt toteuttamaan itsenäisesti opiskellen.”*

5.2 Kurssipäiväkirjojen kokemuksia

Opiskelijoiden tehtävänä oli kirjoittaa omista kannettavan tietokoneen käyttökokemuksistaan langattomalla kampuksella. Seuraavassa on esitetty tämän opetuskokeilun kannalta olennaisimpia opiskelijoiden käyttökokemuksia.

Kurssille osallistuneet opiskelijat olivat havainneet kannettavat tietokoneet hyödyllisiksi opiskelussa. Käyttöpäiväkirjojen perusteella ne nähtiin etuoikeutena erityisesti verkko-opiskelussa. Kannettavan tietokoneen tuoma hyöty opiskelussa ilmeni esimerkiksi luentomuistiinpanojen kirjoittamisessa. Lisäksi koneen omistajuus toi selkeästi esille myös kiinnostuksen sen ylläpitämiseen ja huoltamiseen. Opiskelijoiden kommenteissa korostuivat oman koneen kohdalla omatoimisuus, itse tekeminen ja erilaisten ratkaisujen kokeileminen ongelmatilanteissa.

Kritiikkiä sai osakseen yliopiston infrastruktuuri, sillä opiskelijoiden mielestä yliopiston tiloissa ei ole riittävästi huomioitu kannettavan koneen vaatimia perusominaisuuksia. Esimerkiksi kannettavien akun kesto ei ole riittävä edes luennon ajaksi, mutta koneen akun lataamiseen tarvittavia pistorasiapaikkoja ei ole ollut riittävästi. Tämä nähtiin ongelmana myös uudisrakennuksen kohdalla. Myöskään langaton verkko ei ole saanut opiskelijoita vakuuttumaan langattoman opiskelun eduista. Verkon toimivuus koettiin epävarmaksi, sillä kannettavalla ei aina saa yhteyttä verkkoon.

Käyttöpäiväkirjoista voi havaita, että opiskelijat ovat myös kurssin ulkopuolella pohtineet tietoturvaan liittyviä, luennoilla esiin nousseita asioita. Langattoman verkon tietoturva nähtiin tärkeäksi asiaksi siihen kohdistuvien riskien ja ongelmien osalta. WPA-salausmenetelmän edut havaittiin selkeiksi WEP-salausmenetelmään verrattuna. Kurssin oppeja aiottiin hyödyntää kotiin hankittavalla langattomalla verkolla. Opiskelijat olivat havainneet eroavaisuuksia eri Internet-selainten turvallisuudessa ja käytettävyydessä. Nämä kertovat opiskelijoiden lisääntyneestä tietoturvallisuustietoisuudesta. Opiskelijoiden kommenteista oli havaittavissa tietoturvan huomioiminen oman kannettavan käytössä ja pohdiskelu erilaisten ohjelmien sekä esimerkiksi käyttäjätunnusten ja salasanojen tietoturvallisuudesta. Opiskelijat olivat saaneet lisää tietämystä myös langattomista verkoista ja ymmärsivät niiden toiminnan ja tietoturvan merkityksen niitä käytettäessä.

Opiskelijat pitivät verkkokeskustelua tärkeänä ja onnistuneena opetusmuotona. Verkkokeskustelussa pystyttiin tutustumaan toisten opiskelijoiden ajatuksiin ja osaamiseen, mistä koettiin olevan hyötyä langattoman verkko-opiskeluympäristön tietoturvaa pohtiessa. Asiantuntemusta oli helppo jakaa ja niistä hyötyivät kaikki kurssille osallistuvat. Yhdessä oppiminen koettiin hyväksi tavaksi hankkia uutta tietoa ja hyödyntää toisten käytännön kokemuksia.

Tieto- ja viestintätekniikan opetuskäyttö sai opiskelijoilta myönteisiä kommentteja. Tietotekniikan hyödyntäminen nähtiin voimavarana, jonka yhteydessä kuitenkin mainittiin opetushenkilöstön kielteiset asenteet, puutteelliset resurssit sekä puuttuva osaaminen. Ongelmalliseksi edellä mainittu tilanne havaittiin erityisesti peruskouluissa, jotka muodostavat perustan myöhemmälle oppimiselle.

6 Lähteet

Järvinen, P. 2002. Tietoturva ja yksityisyys. WS Bookwell.
Kalliala, E. Gummerus Kirjapaino Oy. 2002. Verkko-opettamisen käsikirja. Gummerus Kirjapaino Oy.
Magnusson-Sjöberg, C. ym. 2005. IT Law for IT Professionals. Studentlitteratur.
Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Gummerus Kirjapaino Oy.
Opetusministeriön laatukriteerit verkko-opetusmateriaalille. Pdf-dokumentti löytyy osoitteesta: www.edu.fi/julkaisut/laatukriteerit.pdf.
Ruohonen, M. 2002. Tietoturva. WS Bookwell.
Sariola, J. 2003. (toim.) Mobiiliteknologian käyttö ja palvelut yliopistoissa 2003-2006. Mobiiliteknologioiden määrittely Suomen virtuaaliyliopiston palveluihin. Suomen virtuaaliyliopiston e-julkaisuja 7. Julkaisu pdf-dokumenttina osoitteessa: http://www.virtuaaliyliopisto.fi/e-julkaisut/julkaisu007.pdf.
Silander, P. & Koli, H. 2003. Verkko-opetuksen työkalupakki – oppimisaihiosta oppimisprosessiin. Saarijärven Offset Oy.
Tella, S., Vahtivuori, S., Vuorento, A., Wager, P. & Oksanen, U. 2001. Verkko opetuksessa – opettaja verkossa. Edita Oyj.
Thomas, T. 2005. Verkkojen tietoturva – perusteet. Edita Prima Oy.
Tietie-projektin verkkosivut: http://www.helia.fi/tietie/.
Virtuaaliopetuksen haasteet ja niihin vastaaminen 2002. Pdf-dokumentti löytyy sivulta:
http://www.minedu.fi/OPM/Julkaisut/2002/virtuaaliopetuksen_haasteet_ja_niihin_vastaaminen?lang=fi/.
Yliopisto-opetus ja opintoaineistot verkossa. Opintoaineistot verkossa -hankkeen loppuraportti. 31.3.1999. Opetusministeriön koulutuksen ja tutkimuksen tietostrategia – ohjelma: Uudet opetusmenetelmät.Yliopistopaino, Helsinki.

7 Lukumateriaalia

Raportin loppuun on koottu hyödyllisiä linkkejä tietoturvaan, langattomaan verkkoon, opiskeluympäristöihin, verkko-opiskeluun sekä lainsäädäntöön liittyville verkkosivuille sekä kirjallisuus- ja lehtiaineistoja.

Kirjallisuutta ja tieteellisiä aikakauslehtiä
(ks. myös lähteet)

Computers and Security -lehti
Ethics and Information Technology -lehti
Isomäki, Hannakaisa & Hof, Sonja. 2004. Security Concern of Legally Sensitive Web Portals. IEEE Computer Society. 30th EUROMICRO Conference. 544-550.
Järvinen, Petteri. 2003. Salausmenetelmät. Porvoo. WS Bookwell.

Nevgi, A., Kynäslahti, H., Vahtivuori, S., Uusitalo, A. & Ryti, K. 2002. Yliopisto-opettaja verkossa – Taidot puntarissa. Verkko-opettajien osaamisalueiden ja tarjolla olevien tukipalveluiden kartoitus. Helsingin yliopisto. Kasvatustieteen laitos.
Nevgi, A., Löfström, E. & Evälä, A. 2005. (toim.) Laadukkaasti verkossa. Yliopistollisen verkko-opetuksen ulottuvuudet. Kasvatustieteen laitoksen julkaisuja. Julkaisu pdf-dokumenttina osoitteessa:
http://www.helsinki.fi/ktl/julkaisut/lv/laadukkaastiverkossa.pdf/.
Siponen, Mikko T. & Kajava Jorma. 1997. Computer Ethics - Selected Issues Concerning the Morality of Software Piracy. Oulu. Oulun yliopisto.
Thomas, T. 2005. Verkkojen tietoturva – Perusteet. Edita Prima Oy.

Hyödyllisiä verkkosivustoja

ACM: http://www.acm.org/
CERT-FI: www.cert.fi/
European Union Lifelong Learning: http://www.eullearn.net/ebook/
Lapin yliopiston atk-palvelut / opiskelijakannettavat:
http://www.ulapland.fi/opiskelijakannettavat/
McAfeen ohjeistusta:
http://www.jyu.fi/erillis/atkk/palvelut/henkilokunnalle/ohjelmisto/mcafee/mcafee_ohje/
Moodle -opiskeluympäristön opettajan opas:
http://docs.moodle.org/fi/Opettajan_opas/
Opetusministeriö/tekijänoikeus:http://www.minedu.fi/OPM/Tekijaenoikeus/?lang=fi
Oulun yliopiston tietohallinto/kannettavien tietoturva:
http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoa_kannettavat.html/
Roskapostitietoa: http://www.roskapostipaketti.fi/
Suomen lait: http://www.finlex.fi
Suomen virtuaaliyliopisto: http://www.virtuaaliyliopisto.fi/
Tekijänoikeuden tiedotus- ja valvontakeskus ry: http://www.antipiracy.fi/
Tieto- ja viestintätekniikan opetuskäyttö: http://tievie.oulu.fi/verkkopedagogiikka/
Tietosuojavaltuutetun toimisto: http://www.tietosuoja.fi/
Tietotekniikan liitto ry:n jäsenjärjestö: http://www.tietoturva.org/
Tietoturvaopas: http://www.tietoturvaopas.fi/
Tietoyhteiskunnan kehittämiskeskus ry: http://www.tieke.fi/
Tietoyhteiskunnan kehittämiskeskus ry:n tietoturvaopas:
http://www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas/
Verkko-opiskelijan opas: http://www.avoin.jyu.fi/verkko_opiskeluopas/index.htm/
Viestintäviraston tietoturva- ja tietosuojasäädökset:
http://www.ficora.fi/suomi/tietoturva/saadokset.htm/
Virustorjunta: http://www.virustorjunta.net
Yliopistojen tietoturva: http://www.yliopistojentt.uta.fi/index.html/