Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Tietoliikenne

2011

Joni Herranen

MAC OS X JA TIETOTURVA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittely | Tietoliikenne

Marraskuu 2011 | 43 sivua

Ohjaaja: Esko Vainikka

Joni Herranen

MAC OS X JA TIETOTURVA

Tämän opinnäytetyön tavoitteena on luoda kattava kokonaiskuva Mac OS X -käyttöjärjestelmän sisäänrakennetuista tietoturvaratkaisuista ja selvittää miten tietoturvaratkaisut toteuttavat tietoturvan kolmea perustavoitetta eli luottamuksellisuutta, eheyttä ja saatavuutta. Työn kohderyhmäksi on valittu edistyneemmät tietokoneenkäyttäjät, joilla ei ole aikaisempaa Mac-kokemusta.

Teoriaosuudessa syvennytään aluksi Apple-yhtiöön sekä Mac OS X -järjestelmän teknisiin ominaisuuksiin. Osuuden päätavoite on tutustuttaa lukija OS X:n kerrosrakennemalliin ja luoda perustietämys tietoturvasta käsitteenä. Empiiristä osuutta pohjustetaan tutustumalla lyhyesti Mac-konetta uhkaaviin tietoturvauhkiin sekä niitä torjuviin suojamenetelmiin yleisellä tasolla.

Empiirisessä osuudessa tarkastellaan Mac OS X -käyttöjärjestelmän tietoturvaratkaisuja tietojen luottamuksellisuuden, eheyden ja saatavuuden toteuttajina. Tarkastelun kohteena ovat käyttäjätilit ja käyttäjäoikeudet, tiedon salaaminen, haittaohjelmatorjunta, palomuurit, varmuuskopiointi ja salasanahallinta. Lopuksi tutkimuksen havaintojen pohjalta kootaan ytimekäs vinkkipaketti Mac-koneen tietoturvan parantamiseksi.

Apple on selkeästi panostanut tietoturvaratkaisujen helppokäyttöisyyteen. Tästä syystä ratkaisujen läpikäynnissä pääpaino on enemmän esilletuonnissa kuin käytön opastuksessa. Mac OS X:n tietoturvataso on korkea jo oletusasetuksilla käytettäessä, mutta muutamilla toimenpiteillä käyttöjärjestelmän tietoturvapotentiaali voidaan valjastaa vielä tehokkaammin käyttöön.

ASIASANAT:

Mac OS X, tietoturva, CIA-triad, tietoturvan suojamenetelmät

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Datacommunications

November 2011| 43 pages

Instructor: Esko Vainikka

Joni Herranen

MAC OS X AND INFORMATION SECURITY

The objective of this thesis is to create a comprehensive overview of the integrated information security services in the Mac OS X operating system. The primary purpose is to investigate how confidentiality, integrity and availability of information are achieved by using the provided security services. The target audience of this thesis is advanced computer users who have no previous Mac-experience.

In the theoretical part of the thesis the reader is first familiarized with Apple Inc. and the technical properties of the Mac OS X operating system. The main objective of the theoretical part is to create a basic understanding of the layered architecture of Mac OS X and information security as a concept. The most important Mac security threats and security countermeasures at a general level are also briefly discussed.

In the empirical part of the thesis, the integrated information security services of Mac OS X are demonstrated as preservers of confidentiality, integrity and availability. The features which are under the spotlight include user accounts and permissions, data encryption, malware protection, firewalls, backups and password management. Finally, a short guide is created on how to improve Mac-security.

Ease-of-use has been a top priority for Apple when designing the information security services. For that reason, the emphasis of the thesis was on demonstration rather than instruction. The overall security level of Mac OS X is high even with default settings but with minor adjustments the security potential can be tapped into even more efficiently.

KEYWORDS:

Mac OS X, information security, CIA-triad, security countermeasures

SISÄLTÖ

KUVAT

KUVIOT

TAULUKOT

KÄYTETYT LYHENTEET JA SANASTO

AES	Advanced Encryption Standard. Yksi maailman käytetyimmistä salausalgoritmeista. (Kissell 2009, 424.)
DHCP	Dynamic Host Configuration Protocol. Protokolla, jonka tehtävänä on jakaa IP-osoitteet verkkoon kytketyille laitteille.
Dock	Mac OS X-käyttöjärjestelmässä tyypillisesti ruudun alareunassa sijaitseva sovelluskokoelma.
FAT	File Allocation Table. Windowsin tukema tiedostojärjestelmä. (Paananen 2005, 123.)
Finder	Mac OS X:n tiedostojen ja kansioiden selaamisympäristö.
FireWire	Nopea oheislaiteliitäntätyyppi. Käytetään esimerkiksi digikameroiden tiedonsiirtoon. (Paananen 2005, 460.)
HFS+	Hierarchical File System Plus. Mac OS X:n käyttämä tiedostojärjestelmä. (Barker ym. 2010, 94.)
Palvelunestohyökkäys	Tarkoituksena kuormittaa kohdetietokone tai palvelin valtavalla määrällä hakupyyntöjä, jotta kohde ei pystyisi enää toimimaan normaalisti (Paananen 2005, 396).
Plug and Play	Ominaisuus, jossa oheislaite on käyttövalmis välittömästi, kun se on liitetty tietokoneeseen (Merriam Webster 2011).
Porttaus	Sovelluksen muuttaminen toiseen käyttöjärjestelmään tai ympäristöön sopivaksi.
POSIX	Portable Operating System Interface. Unix-käyttöjärjestelmien peruskäytäntöjä koskeva standardikokoelma. (Barker ym. 2010, 80.)
Pääte	Mahdollistaa tietokoneen kanssa kommunikoinnin erilaisten käskyjen avulla. Englanniksi ”Terminal”.
Syöttölaite	Laite, jonka avulla käyttäjä syöttää tietoja tietokoneelle. Esimerkiksi hiiri ja näppäimistö ovat syöttölaitteita.
Unix	Laitteisto- ja valmistajariippumaton avoin käyttöjärjestelmä. Suosittu palvelintietokoneissa ja suurkoneympäristöissä. (Paananen 2005, 143.)
Vapaa lähdekoodi	Ohjelmointitapa, jossa lähdekoodi on kaikkien nähtävillä. Kuka tahansa voi muokata ja jakaa ohjelmaa eteenpäin. (Paananen 2005, 455.)

1 JOHDANTO

Applen Mac-tietokoneiden suosio on kasvanut räjähdysmäisesti viime vuosina. Tuloksena IT-alalle on syntynyt kiivas kilpailutilanne pitkään markkinoita hallinneen Microsoftin ja Applen käyttöjärjestelmien kesken. Järjestelmiä vertailtaessa erityisesti tietoturva-asiat ovat olleet suurennuslasin alla. Applen Mac OS X:n tietoturva on yleisesti todettu paremmaksi kuin Microsoftin Windows-käyttöjärjestelmän.

Mutta mitkä ominaisuudet tekevät Mac OS X:stä tietoturvallisemman? Suomenkielinen aineisto aiheesta on melko suppeaa ja hajanaista. Opinnäytetyön tavoitteena on selvittää miten tietoturvallisuus varmistetaan Mac OS X:ssä. Käytännössä tämä tapahtuu tarkastelemalla käyttöjärjestelmän tietoturvaratkaisuja. Teoreettisen viitekehyksen tutkimukselle tarjoaa tietoturvan perusperiaate CIA-triad. Pääpaino on selvittää miten CIA-triadin kolme osa-aluetta eli luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability) toteutuvat OS X -käyttöjärjestelmässä. Lopuksi tutkimuksen havaintojen pohjalta kootaan ytimekäs vinkkipaketti kotikäyttäjille Mac-tietokoneen tietoturvan parantamiseksi. Tietoturvaosuutta pohjustetaan perinpohjaisella katsauksella Apple-yhtiöön sekä Mac OS X:n taustoihin ja teknologioihin. Päällimmäisenä pyrkimyksenä on tutustuttaa lukija OS X:n kerrosrakennemalliin, jonka sisältämät ratkaisut etenkin alemmilla tasoilla vaikuttavat väistämättömästi myös tietoturvaan.

Opinnäytetyö on tehty Mac OS X 10.6 Snow Leopard -version pohjalta. Syitä tähän valintaan ovat käyttöjärjestelmän suosio ja kirjallisuustarjonta. Opinnäytetyön teoria ja käytäntö ovat kuitenkin täysin sovellettavissa myös OS X:n versioon 10.5 Leopard ja osittain versioon 10.7 Lion.

Lähteiden arvioimisen kannalta työ on melko haastava. PC- ja Mac-tietokoneiden kilpailuasetelman johdosta tietokoneenkäyttäjät ovat jakautuneet kahteen leiriin. Osa Mac-käyttäjistä on hyvinkin fanaattisia, mikä laskee heidän tekstiensä lähdearvoa. Opinnäytetyön tekijänä en halua kuulua edellä

mainittuun joukkoon, joten työn näkökulma on pyritty pitämään neutraalina. Tekstistä hyötyvät parhaiten edistyneemmät tietokoneenkäyttäjät, jotka ovat ensimmäistä kertaa vaihtamassa Mac OS X-järjestelmään. Tämä ei kuitenkaan tarkoita, että vasta-alkajille opinnäytetyö olisi hyödytön. Etenkin tietoturvaosuus on kirjoitettu siten, että myös aloittelijat pystyvät tutustumaan tietoturvan perusteisiin sekä OS X:n tarjoamiin tietoturvapalveluihin.

2 APPLE MAC OS X-KÄYTTÖJÄRJESTELMÄ

2.1 Apple-yhtiö

Apple Inc. on yhdysvaltalainen kulutuselektroniikkatuotteiden, tietokoneiden ja tietokoneohjelmien valmistaja. Omenalogostaan tunnetun yhtiön perustivat vuonna 1976 Applen edesmennyt toimitusjohtaja Steve Jobs yhdessä Steve Wozniakin kanssa. Applen yksi kuuluisimpia laitteita on 1980-luvulla kehitetty Macintosh-tietokone, joka mullisti henkilökohtaisten tietokoneiden suunnittelun. Macintosh-koneet toivat ensimmäisinä markkinoille graafisen käyttöliittymän, jossa navigointi tapahtuu hiirellä napsauttamalla. (Brown 2000, 78-81.)

Vanhojen Macintosh-laitteiden perinteitä nykypäivänä jatkavat iMac, Mac Pro ja Mac Mini -pöytätietokoneet. Pöytätietokoneiden rinnalla Apple valmistaa myös kannettavia tietokoneita eri käyttötarkoituksiin. MacBook-mallisto on suunnattu kotikäyttäjille ja MacBook Pro -sarja ammattikäyttäjille. Ammattikäyttöön Apple tarjoaa lisäksi ohutta MacBook Air -kannettavaa. (Reuters 2011.) Kaikissa koneissa on valmiiksi asennettuna Applen oma Mac OS X-käyttöjärjestelmä. Lisäksi palvelinkoneille on olemassa oma versionsa Mac OS X:stä.

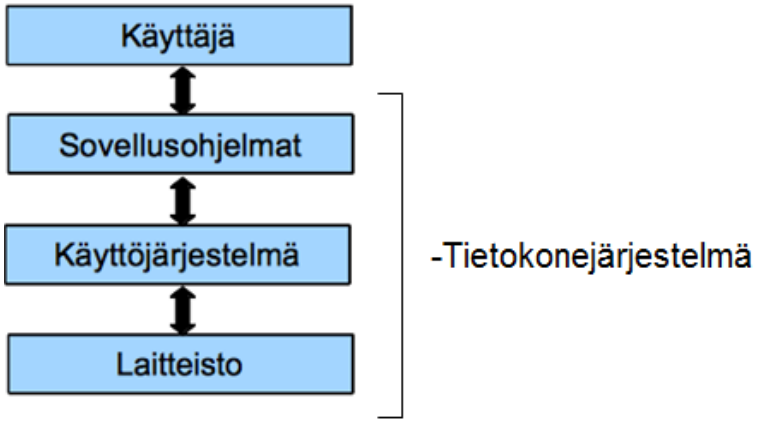
Applen kulutuselektroniikkatuotteista suosituimpia ovat iPhone-älypuhelin, iPod-musiikkisoitin ja iPad-taulutietokone. IPhone-puhelin yhdistää matkapuhelimen, musiikkisoittimen ja internetin yhdeksi kämmenenkokoiseksi laitteeksi. IPad on suunniteltu kokonaisvaltaiseksi mediasoittimeksi, jonka avulla videoiden ja kuvien katselu sekä pelaaminen onnistuu helposti. Myös iPodilla on mahdollista katsella videokuvaa, mutta pienen kokonsa vuoksi soitin soveltuu parhaiten pelkästään musiikin kuunteluun. Kaikkiin edellä mainittuihin laitteisiin on asennettu iTunes-musiikkisoitinohjelma, jonka avulla voi musiikinkuuntelun ohella ostaa ja vuokrata mm. digitaalista musiikkia, äänikirjoja, elokuvia ja TV-sarjoja. (Reuters 2011.)

Applen tuotteet ovat saavuttaneet valtavan suosion erityisesti nuorison keskuudessa. Jotkut ovat alkaneet puhua jopa Apple-kultista (Mitchell 2007).

Applen puolestapuhujat korostavat usein tuotteiden ainutlaatuista designia ja helppokäyttöisyyttä. Apple Inc. ohittikin Microsoftin maailman suurimpana teknologiayhtiönä markkina-arvolla mitattuna vuonna 2007 (Rigby 2010).

2.2 Yleistä Mac OS X:stä

Käyttöjärjestelmällä tarkoitetaan joukkoa pienohjelmia, joiden avulla tietokonetta ja sen resursseja hallitaan. Varsinaisessa työskentelyssä käytettävät sovellusohjelmat, kuten internetselaimet ja tekstinkäsittelyohjelmat, toimivat käyttöjärjestelmän alaisuudessa. Käyttöjärjestelmä mahdollistaa sovellusohjelmien käytön suorittamalla erilaisia perustehtäviä. Lyhyesti sanottuna käyttöjärjestelmä toimii linkkinä käyttäjän, sovellusten ja laitteiston välillä kuvion 1 mukaisesti. (Paananen 2005, 132.)



Kuvio 1. Tietokonejärjestelmän ja käyttäjän rajapinnat (Paananen 2005, 132).

Mac OS X -käyttöjärjestelmä on esiasennettu kaikkiin Applen Macintosh-tietokoneisiin. Käyttöjärjestelmän nimessä esiintyvä X-kirjain viittaa roomalaiseen numeroon kymmenen. Eri versiot on nimetty kissaeläinten mukaan. Esimerkiksi heinäkuussa 2011 julkaistua 10.7-versiota kutsutaan nimellä “Lion” (Leijona). Lisäksi 10.6 “Snow Leopard”- ja 10.5 “Leopard”-versiot ovat vielä laajalti käytössä. Mac OS X Snow Leopard sijoittuu käytetyimpien käyttöjärjestelmien listalla neljänneksi Microsoft Windowsin hallitessa kärkikolmikkoa (StatOwl.com 2011).

2.3 Tekniset ominaisuudet

Yksinkertaisimmillaan Unix-pohjaista Mac OS X-käyttöjärjestelmää voidaan kuvata kerrosmallilla (kuvio 2). Alemmilla kerroksilla sijaitsevat tietokoneen toiminnan kannalta tärkeät toiminnot, joihin ylemmän kerroksen palvelut, tekniikka ja sovellukset tukeutuvat. Tavallinen tietokoneenkäyttäjä näkee tavallisesti vain ylimpänä sijaitsevan kerroksen, joten kerrosmallin konkreettiset hyödyt eivät ole selkeästi nähtävissä. Mac OS X on kuitenkin hyvin joustava käyttöjärjestelmä, josta hyötyvät etenkin ohjelmistokehittäjät. Eri kerroksilla sijaitsevat teknologiat on suunniteltu toimimaan tehokkaasti yhdessä (kuvio 2). (Apple Inc. 2009, teknologiadokumentaatio.)

Kuvio 2. Mac OS X-kerrosmalli (Apple Inc. 2009, teknologiadokumentaatio).

2.3.1 Darwin-ydin

Mac OS X-käyttöjärjestelmän peruskivenä toimii Unix-pohjainen Darwin. Mac OS X:n mainostettu vakaus kumpuaa juuri Darwinista, joka on suunniteltu luotettavaksi ja suorituskykyiseksi järjestelmäksi. Darwinin sisältä löytyy Mach 3.0 -mikrokernel, joka hallinnoi tietokoneen suoritinta ja muistin käyttöä. Mach priorisoi prosesseja ja huolehtii siitä, että niillä on riittävät suoritinresurssit. Suorituskyvyn tehostamiseksi prosessit voidaan jakaa suorittimen eri ytimien kesken. Muistinkäytön optimoinnilla sovellukset eristetään toisistaan ja järjestelmän kannalta tärkeistä prosesseista. Tämä mahdollistaa sen, että yksi “huonosti käyttäytyvä” ohjelma ei pysty kaatamaan koko käyttöjärjestelmää.

Lisäksi Mach-kerneliin on ohjelmoitu edistyneitä muistinhallintatekniikoita: keskusmuistissa sijaitseva käyttämätön tieto voidaan siirtää kiintolevylle kipeästi keskusmuistia tarvitsevien sovellusten tieltä. (Clancy ym. 2008, 5; Apple Inc. 2009, teknologiadokumentaatio.)

Kernelin hallitessa suoritinta ja muistia yleisellä tasolla, laiteajurit mahdollistavat kommunikoinnin erilaisten valmistajien ja mallien kanssa. Darwin tarjoaa laiteajurien kehittäjille erillisen sovelluskehyksen, joka mahdollistaa muun muassa plug and play- ja virransäästöominaisuudet. Sovelluskehyksen etu on se, että tukea uudelle laitteelle ei tarvitse ohjelmoida suoraan kerneliin. Darwin sisältää myös lukuisia oletusajureita tietokoneen peruskomponenteille, joten kotikäyttäjän ei juurikaan tarvitse huolehtia erillisten ajureiden asentamisesta. (Apple Inc. 2009, teknologiadokumentaatio; McCormack & Trent 2010, 8.)

2.3.2 Grafiikka ja media

Kerrosmallissa ytimen yläpuolella sijaitsee grafiikka- ja mediakerros. Se sisältää työkalut kaksiulotteisen, kolmiulotteisen ja videopohjaisen sisällön piirtämiseen. Järjestelmä tarjoaa myös tuen monikanavaisen äänen toistamiseen, muokkaamiseen ja luomiseen. (Apple Inc. 2009, teknologiadokumentaatio.)

Mac OS X:n yksi tärkeimmistä grafiikkateknologioista on Quartz. Quartz huolehtii työpöydän ikkunoiden sijoittelusta ja yleisesti grafiikoiden oikeanlaisesta piirtämisestä. Syöttölaitteiden avulla annettujen käskyjen välittäminen ydinkerrokselta sovelluskehyskerrokseen on myös Quartzin vastuulla. Kaksiulotteisen grafiikan moottorina toimii Quartz 2D -kirjasto, jossa on myös sisäänrakennettu tuki PDF-tiedostojen näyttämiseen ja luomiseen. (McCormack & Trent 2010, 13-15.)

Kaksiulotteisen grafiikan piirtämisessä Quartzia tukee OpenGL-kirjasto. Suorituskykynsä ansiosta OpenGL soveltuu kuitenkin parhaiten 3D-grafiikan mallintamiseen esimerkiksi tietokonepeleissä, videoeditoinnissa ja tieteellisessä tutkimustyössä. Suurin osa OpenGL:n komentojen laskentatyöstä suoritetaan suoraan näytönohjaimessa, joten suoritin voi rauhassa keskittyä muihin prosesseihin. (McCormack & Trent 2010, 15.)

Quicktime on Applen kehittämä teknologia videokuvan, valokuvien ja äänen käsittelyyn ja toistamiseen. Uusi Quicktime X-versio on suunniteltu valjastamaan uusimpien Mac-koneiden moniydinprosessorit ja ohjelmoitavat näytönohjaimet mahdollisimman tehokkaasti käyttöönsä. Mac OS X hyödyntää Quicktimea vahvasti käyttöliittymässään ja verkkoliitännäisissä sovelluksissaan. (McCormack & Trent 2010, 15-16.)

Quicktimea monipuolisemmat välineet monikanavaisen äänen käsittelyyn tarjoaa Core Audio -sovelluskehys. Core Audiota voidaan käyttää ääni- ja MIDI-tiedostojen toistamiseen, luomiseen, editoimiseen ja äänittämiseen. Lisäksi sovelluskehys tarjoaa tarvittavat palvelut USB- ja FireWire-pohjaisten audiolaitteiden liittämiseen. (Apple Inc. 2009, teknologiadokumentaatio.)

2.3.3 Sovelluskehykset

Mac OS X-käyttöjärjestelmän toiseksi ylin kerros eli sovelluskehyskerros on ohjelmistokehittäjien toiminta-aluetta. Sovelluskehykset koostuvat käyttöjärjestelmän tarjoamista resursseista, komponenteista ja palveluista, jotka yhdessä mahdollistavat sovelluksen toiminnan (Clancy ym. 2008, 6). Mac OS X tarjoaa lukuisia sovelluskehyksiä, joista jokainen soveltuu erilaisiin ohjelmointitarkoituksiin (Apple Inc. 2009, teknologiadokumentaatio).

Cocoa-sovelluskehystä hyödyntävät sovellukset on suunniteltu varta vasten Mac OS X:lle. Kyseiset sovellukset eivät toimi Mac OS 9:ssä ja sitä vanhemmissa käyttöjärjestelmissä. Cocoa pyrkii vastaamaan modernin olio-ohjelmoinnin ja nopeatahtisen ohjelmistokehityksen vaatimuksiin valjastamalla Darwin-kernelin koko potentiaalin käyttöönsä. Tuloksena on nopea ja helppokäyttöinen ympäristö, joka sopii hyvin kokemattomille ohjelmoijille. (Clancy ym. 2008, 7; Apple Inc. 2009, teknologiadokumentaatio.)

Cocoan tarjotessa valmiin koodin joillekin sovellusominaisuuksille, jää ohjelmistokehittäjien omalle luovuudelle vähemmän tilaa. Ohjelmoijan halutessa vapaat kädet koodin suhteen Carbon-ympäristö antaa tähän mahdollisuuden. Carbon soveltuu hyvin sovelluksien porttaamiseen vanhoista Mac-käyttöjärjestelmistä uuteen Mac OS X Snow Leopardiin. Kaikesta huolimatta

Apple suhtautuu Carboniin melko nuivasti johtuen sen kykenemättömyydestä toimia tehokkaasti nykyaikaisten laitteistojen ja ohjelmistojen kanssa. (Apple Inc. 2009, teknologiadokumentaatio; McCormack & Trent 2010, 18.)

Tietokoneenkäyttäjille tutuin Mac OS X:n sovelluskehyksistä lienee Java. Javan suurin vahvuus on se, että Java-sovellukset toimivat monissa erilaisissa ympäristöissä ja laitteistoissa. Tämänkaltaisella monipuolisuudella on kuitenkin huonot puolensa: Javalla työskenneltäessä ohjelmistokehityksen painopiste on laitteistoriippumattomissa ominaisuuksissa. Mac OS X:lle yksilöityjä teknologioita on siis vaikea ottaa käyttöön, sillä muissa ympäristöissä kyseisiä teknologioita ei ole. (McCormack & Trent 2010, 19.)

2.3.4 Käyttäjäkokemus

Mac OS X:n käyttöliittymää kutsutaan nimellä Aqua. Aqua määrittää käyttöjärjestelmän ikkunoiden ja valikoiden ulkonäön ja yleisen käyttäytymisen. Applen mukaan käyttöliittymän tavoitteena on yhdistää värit, läpikuultavuus ja monimutkaiset tekstuurit silmää miellyttäväksi kokonaisuudeksi. Apple Human Interface Guidelines -ohjeisto määrittelee sovellusten käyttöliittymien vaatimukset. Ohjelmistojen samannäköisyys helpottaa niiden käyttöä ja luo vaikutelman, että ohjelmat on suunniteltu toimimaan yhdessä käyttötarkoituksesta riippumatta. (McCormack & Trent 2010, 19; Apple Inc. 2011.)

3 TIETOTURVALLISUUDEN PERUSKÄSITTEITÄ

Yleisesti tietoturva viittaa kaiken sellaisen tiedon suojaamiseen, jolla on arvoa ihmiselle, yritykselle tai organisaatiolle. Tyypillisesti arvokas tieto on elektroninen tai paperinen dokumentti, mutta myös laitteiston tai ohjelmiston asetustiedot ja tietoliikennedata vaativat suojausta. Tietokoneita ja tietojärjestelmiä kutsutaan tietoa sisältäviksi suojattaviksi kohteiksi (Information assets). Yrityksille tietoturva on liiketoiminnan jatkuvuuden kannalta elintärkeää, mutta myös yksityishenkilöiden tulisi ottaa tietoturvallisuusasiat vakavasti.

Yleinen harhaluulo on, että tietoturvallisuus on pelkästään tietokoneiden parissa työskentelyä. Tosiasiassa ihmisiin kohdistettu tietoturvatoiminta on tärkeämpää. Tietämättömyys ja välinpitämätön asenne tietoturva-asioita kohtaan tekevät ihmisestä ketjun heikoimman lenkin. Perinteisesti tietoturva on jaettu taulukossa 1 esitettyihin osa-alueisiin:

Taulukko 1. Tietoturvan osa-alueet (Valtiovarainministeriö 2003, 39-51).

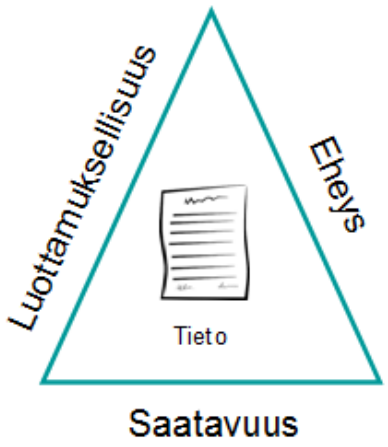
Osa-alue	Kuvaus
Hallinnollinen tietoturva	Tietoturvaperiaatteiden suunnittelu, luonti ja hallinnointi organisaatiossa
Henkilöstöturvallisuus	Henkilöstöön liittyvien riskien hallinta koskien mm. soveltuvuutta, toimenkuvaa, tiedon käyttöoikeuksia ja turvallisuuskoulutusta
Fyysinen turvallisuus	IT-laitteiden ja tietovarastojen suojelu fyysisiltä tapaturmilta ja vahingoittamisyrityksiltä
Tietoliikenneturvallisuus	Verkon kautta välitettävien tietojen turvaaminen ja verkkoon liitettyjen laitteiden suojelu murtautumisyrityksiltä
Laitteistoturvallisuus	IT-laitteiden käytettävyyden ja toiminnan varmistaminen
Ohjelmistoturvallisuus	Ohjelmistoversioiden ja lisenssien hallinta sekä sovelluksien tietoturvan laadunvarmistus
Tietoaineistoturvallisuus	Tietojen ja tietoja sisältävien järjestelmien luottamuksellisuuden, eheyden ja saatavuuden takaaminen
Käyttöturvallisuus	Tietotekniikan turvallisen käytön varmistaminen sisältäen mm. käyttäjätunnukset ja salasanat sekä virustorjunnan

Osa-aluejaon merkitys korostuu etenkin yritysmaailmassa, mutta luokittelua voi soveltaa myös yksityishenkilön tietoturva-asioihin. Käyttöjärjestelmän tietoturvaa tarkasteltaessa liikutaan lähinnä tietoaineistoturvallisuuden,

tietoliikenneturvallisuuden ja käyttöturvallisuuden alueilla. On kuitenkin huomattava, että eri osa-alueet eivät ole kovinkaan selvärajaisia. Esimerkiksi käyttöturvallisuuteen liittyviä asioita voidaan helposti sisällyttää muihin osa-alueisiin.

Tietoturvan tavoitteena on taata tietojen ja tietoja sisältävien suojattavien kohteiden luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability). Yhdessä nämä tukipilarit muodostavat peruskäsitteen, jota kutsutaan nimellä CIA-triad (kuvio 3). Salainen dokumentti on tietoturvallinen vasta sitten, kun kaikki CIA-triadin tukipilarit toteutuvat.

Luottamuksellisuudella tarkoitetaan, että tieto on vain sen käsittelyyn oikeutettujen henkilöiden saatavilla. Luottamuksellisuutta ei kuitenkaan voida ylläpitää ilman tiedon eheyttä. Eheyden toteutuessa voidaan olla varmoja siitä, että tieto on varmasti totuudenmukaista ja vain oikeutettujen henkilöiden tarkoituksellisesti muokattavissa. Saatavuus tarkoittaa, että tieto on aina viiveettömästi käytettävissä kun sitä tarvitaan. (Paananen 2005, 387-388; Chapple ym. 2008, 181.)



Kuvio 3. CIA-triad ja tietoturvallinen dokumentti (Information Systems Security Working Group 2011).

4 TIETOTURVARATKAISUT MAC OS X:SSÄ

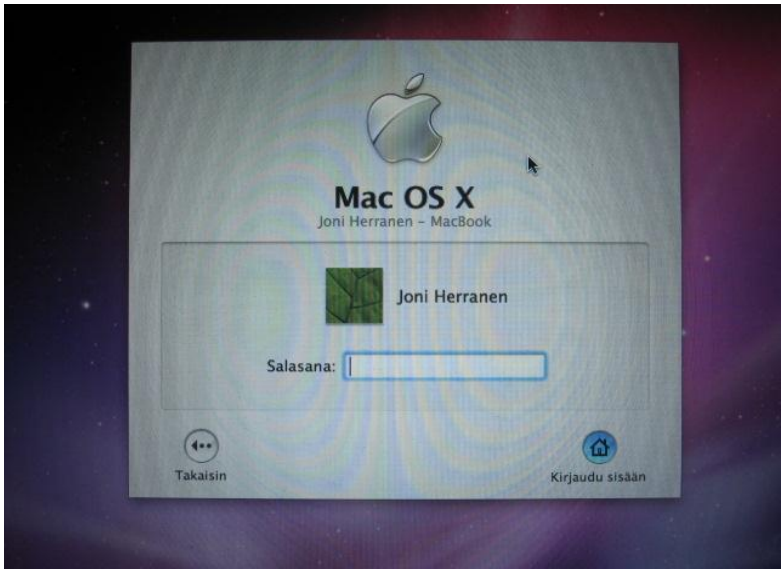
Tietoturvallisuuden saavuttamiseksi on määriteltävä, millaisia suojatoimenpiteitä erilaisia tietoturvauhkia vastaan käytetään, jotta CIA-triadin tukipilarit toteutuvat. On tärkeää huomata, että yksittäinen tietoturvauhka voi vaarantaa yhden sijasta kaikki tukipilarit. Vastaavasti hyvä tietoturvaratkaisu pystyy torjumaan useampaan kuin yhteen CIA-triadin tukipilariin kohdistuvia uhkia.

Kotikäyttäjien tarpeisiin Mac OS X-käyttöjärjestelmään on tarjolla lukuisia tietoturvapalveluita, joiden esittelyyn tässä luvussa pääasiassa keskitytään. Suurin osa palveluista on sisäänrakennettuna suoraan käyttöjärjestelmään. Ainoastaan virustorjunnan laaja-alainen turvaaminen vaatii ulkopuolisen ohjelmiston.

4.1 Luottamuksellisuus

4.1.1 Käyttäjätilit ja käyttäjäoikeudet

Jos luottamuksellisuus ei toteudu, pahimmassa tapauksessa tieto tai tietoa sisältävä suojattava kohde voi olla kaikkien sellaisten henkilöiden saatavilla, joilla ei ole oikeutta käsitellä kohdetta. Tietojen käyttöä voidaan rajoittaa käyttöjärjestelmän pääsynvalvonnalla luomalla salasanalla varustettuja yksilöityjä käyttäjätilejä (kuva 1). Pääsynvalvonta jakautuu kolmeen osaan: tunnistukseen (Identification), todennukseen (Authentication) ja oikeutukseen (Authorization). Tunnistuksessa määritetään käyttäjän henkilöllisyys annetun käyttäjänimen perusteella. Todennuksessa käyttäjänimeen liitetyllä salasanalla henkilöllisyys varmistetaan. Oikeutus määrittää käyttäjän käyttöoikeudet järjestelmän sisältämiin tietoihin. Kunnollisella pääsynvalvonnalla voidaan tietojen luottamuksellisuus turvata sekä sisäisiltä että ulkoisilta uhilta. Yrityksissä sisäisen uhan muodostavat omat työntekijät, jotka tahattomasti tai tahallisesti omasta uteliaisuudestaan käsittelevät tietoja, joihin heillä ei ole oikeuksia. Ulkoinen uhka voi olla esimerkiksi tietojärjestelmään murtautuva hakkeri tai tietokoneen varastava pahantekijä. Jos hakkeri tai rosvo ei tiedä käyttäjätunnusta ja salasanaa, koneelle ei voi kirjautua (Paananen 2005, 398).



Kuva 1. Mac OS X:n sisäänkirjautumisruutu.

Mac OS X:ssä voidaan erottaa kuusi erilaista käyttäjätilityyppiä, jotka ovat ylläpitäjä, normaali, käyttörajoitusten alainen, vieras ja vain jako. Kuudes tilityyppi on juurikäyttäjä eli root, mutta se on oletusasetuksissa poistettu käytöstä. Käyttörajoitusten alainen, vieras ja vain jako ovat käytännössä normaali-tilin alalajeja. (Kissell 2009, 62.) Uusien käyttäjien lisääminen ja käyttäjätilien hallinta tapahtuu järjestelmäasetuksissa sijaitsevan “Käyttäjät” -ikkunan kautta.

Ylläpitäjä (Administrator) on henkilö, joka huolehtii tietokoneen toiminnasta. Ylläpitäjätilillä voi muuttaa lähes kaikkia koneen asetuksia ja määritellä muiden käyttäjien oikeuksia. Koska Mac OS X on Unix-pohjainen käyttöjärjestelmä, jokaisella Mac-koneella on oltava vähintään yksi ylläpitäjätili. Ensimmäinen ylläpitäjätili luodaan jo käyttöjärjestelmän asennusvaiheessa. Ylläpitäjätilin omaavalla henkilöllä on oikeus

- omaksua juurikäyttäjän oikeudet
- asentaa ohjelmia kaikille käyttäjille
- muuttaa kaikkia käyttäjiä koskevia järjestelmäasetuksia
- luoda, muokata ja poistaa käyttäjätilejä. (Kissell 2009, 62-63.)

Mac OS X:ssä ei ole valmiina normaaleja käyttäjätilejä, joten ylläpitäjän on itse luotava ne. Normaalitilin oikeuksilla voidaan tehdä samoja asioita kuin

ylläpitäjätilillä, mutta muutosoikeudet koskevat ainoastaan omaa tiliä. Normaalitilin omaava henkilö voi siis

- lukea, muokata ja poistaa omia tiedostojaan
- asentaa ohjelmia omaan käyttöön
- muuttaa omaa tiliä koskevia järjestelmäasetuksia. (Kissell 2009, 64.)

Käyttörajoituksien alaiselle tilille (Managed account) on nimensä mukaisesti asetettu tietokoneen käyttöä koskevia rajoitteita. Rajoitteet voivat olla hyödyksi esimerkiksi lapsiperheissä sekä työpaikoilla. Ylläpitäjä pystyy määrittämään käyttäjälle sallitut ja kielletyt sovellukset sekä rajoittamaan internetin käyttöä. Aikuisille tarkoitetuille sivustoille pääsy on mahdollista estää automaattisesti tai ylläpitäjä voi sallia vierailut vain tietyille verkkosivustoille. Lisäksi Mail-sovelluksella suoritettava sähköpostiviestintä ja iChat-pikaviestikeskustelut voidaan rajoittaa vain sallittujen henkilöiden osoitteisiin. Aikarajoituksilla tietokoneen käytölle pystytään asettamaan maksimituntimäärä erikseen arkipäiville ja viikonlopuille. Pääsy tietokoneelle voidaan myös estää tiettyinä vuorokaudenaikoina. Ylläpitäjä pystyy seuraamaan käyttörajoitettujen tilien käyttöä lokitiedoista. Järjestelmä kerää tietoja vierailluista verkkosivuista, kiellettyjen sivustojen vierailuyrityksistä, käytetyistä ohjelmista ja iChat-keskusteluista.

Vierastilin avulla voidaan tietokonetta satunnaisesti käyttäville henkilöille antaa oikeudet kirjautua koneelle. Näin jokaiselle tilapäiselle käyttäjälle ei tarvitse erikseen luoda omaa käyttäjätiliä. Aivan kuten käyttörajoituksien alaisessa tilissä, ylläpitäjä voi asettaa vierastilille edellä läpikäytyjä käyttörajoituksia ja valvoa tilin käyttöä lokitiedoista. Vierastilille kirjautumiseen ei tarvita salasanaa ja uloskirjautumisen yhteydessä kaikki tilin tiedot ja tiedostot poistetaan.

Vain jako-tilin avulla käyttäjälle annetaan oikeudet päästä käsiksi tietokoneen jaettuihin resursseihin. Näitä jaettuja resursseja ovat näytön jakaminen, tiedostonjako, etäkirjautuminen, Apple Remote Desktop -etähallinta ja Apple Event -etäkomennot. Resursseja ja niihin oikeutettuja käyttäjiä voidaan hallita järjestelmäasetuksissa sijaitsevan “Jako”-ikkunan kautta. Vain jako-tilin avulla

kohdekoneelle voidaan kirjautua ainoastaan etänä verkon kautta. (Kissell 2009, 66.)

Viimeinen tilityyppi on juurikäyttäjä eli root. Juurikäyttäjällä on samat oikeudet kuin ylläpitäjällä, mutta muutamalla lisäominaisuudella varustettuna. Mac OS X sisältää ylläpitäjiä koskevia turvamekanismeja, joiden tarkoitus on estää väärinkäytökset, jos ylläpitäjätili joutuu vääriin käsiin. Muutettaessa tiettyjä järjestelmäasetuksia ylläpitäjää pyydetään tunnistautumaan syöttämällä tilin salasana. Juurikäyttäjä ohittaa nämä turvamekanismit ja pystyy siten vapaasti muuttamaan tietokoneen asetuksia ja muokkaamaan tiedostoja. Rajattomilla oikeuksilla juurikäyttäjä voi myös vahingoittaa tietokonetta tahallisesti tai tahattomasti esimerkiksi poistamalla järjestelmän toiminnan kannalta tärkeitä tiedostoja. Tästä johtuen root-tili on oletuksena kytketty pois päältä. Kotikäyttäjän ei tarvitse, eikä kannata koskaan aktivoida root-tiliä, sillä sen käyttämiseen liittyy huomattavia tietoturvariskejä. (Kissell 2009, 67.)

Jokaisella ylläpitäjän luomalla käyttäjätilillä on oma kotikansio Mac-koneen kovalevyllä. Kotikansio sisältää tallennustilan muun muassa käyttäjän henkilökohtaisille asetuksille, dokumenteille, kuville ja tiedostolatauksille. Kotikansiot ovat pääosin yksityisiä - ainoastaan root-käyttäjä pystyy tarkastelemaan muiden käyttäjien tiedostoja.

Mac OS X -käyttöjärjestelmässä jokaisella kansiolla ja tiedostolla on omistaja ja tietynlaiset käyttöoikeudet. Uusimmat käyttöjärjestelmäversiot seuraavat POSIX-standardin mukaisia käyttöoikeuksia. POSIX-käyttöoikeutuksessa käyttäjille voidaan antaa tiettyyn kansioon tai tiedostoon kolme erilaista toimintoa; read eli luku, write eli kirjoitus ja execute eli suoritus. Toiminnot lyhennetään kirjaimin “r”, “w” ja “x”. “Read” tarkoittaa, että käyttäjä voi avata tiedoston ja tarkastella sen sisältöä. “Write” -toiminto antaa tiedoston tai kansion muokkaus- ja poisto-oikeuden. “Execute” -toiminto oikeuttaa sovelluksen käynnistämiseen ja kansion sisällön listaamiseen. (Kissell 2009, 52.)

Yksittäisen käyttäjän oikeudet merkitään kolmen kirjaimen joukkona, jossa kirjaimien paikat ovat aina samat. Esimerkiksi jos käyttäjällä on tiedostoon luku-,

kirjoitus- ja suoritusoikeudet, käyttöoikeudet merkitään muotoon “rwx”. Jos jonkin toiminnon paikalla on “-” -merkintä, käyttäjällä ei ole oikeuksia suorittaa kyseistä toimintoa. (Kissell 2009, 52.) Esimerkkinä luku- ja kirjoitusoikeudet merkitään “rw-” ja vain luku -oikeudet “r--”.

Tiedoston tai kansion täydelliset käyttöoikeudet koostuvat kolmesta kolmen kirjaimen joukosta. Tutut “r”, “w” ja “x” -toiminnot ovat edelleen voimassa, mutta ne viittaavat erilaisiin käyttäjiin (kuva 2). Ensimmäinen joukko koskee tiedoston tai kansion omistajaa, toinen joukko tiedoston tai kansion omistavaa ryhmää ja kolmas kaikkia muita käyttäjiä. (Kissell 2009, 53.) Ryhmien luominen on kätevä tapa antaa tietyille käyttäjille käyttöoikeuksia haluttuihin tiedostoihin.

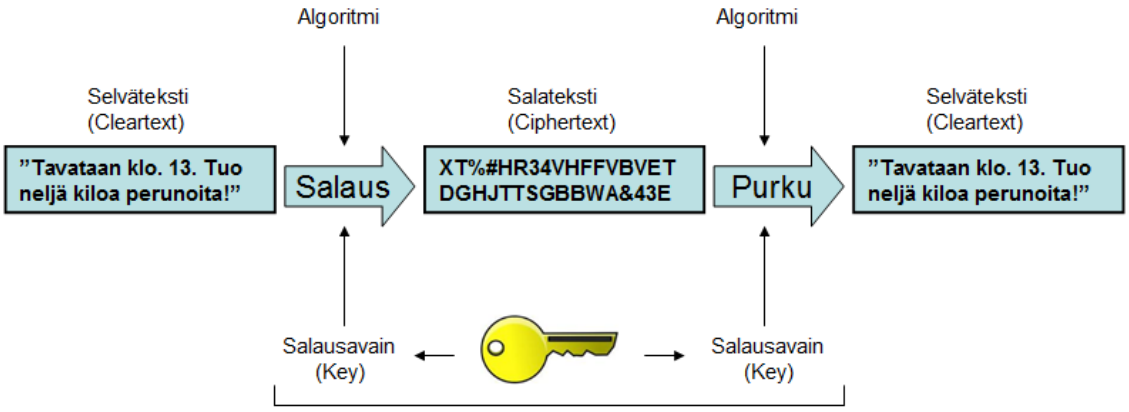
```
Last login: Fri Sep  9 10:00:49 on console
Joni-Herranen-MacBook:~ Joni$ ls -l
total 0
drwx------+  4 Joni  staff   136 31 Elo 10:36 Desktop
drwx------+  8 Joni  staff   272 24 Elo 16:43 Documents
drwx------+ 15 Joni  staff   510  8 Syy 12:34 Downloads
drwx------+ 38 Joni  staff  1292  6 Syy 22:38 Library
drwx------+  3 Joni  staff   102 16 Kes 17:27 Movies
drwx------+  5 Joni  staff   170 24 Hei 18:16 Music
drwx------+ 11 Joni  staff   374 24 Elo 23:10 Pictures
drwxr-xr-x+  6 Joni  staff   204 17 Kes 00:29 Public
drwxr-xr-x+  6 Joni  staff   204 19 Kes 22:53 Sites
Joni-Herranen-MacBook:~ Joni$
```

Kuva 2. Kotikansion käyttöoikeuksien tarkastelu päätteen avulla.

Esimerkiksi kuvassa 2 “Sites”-kansion omistaja on käyttäjä “Joni” ja hänellä on kansioon luku-, kirjoitus- ja suoritusoikeudet. “Staff”-ryhmällä on luku- ja suoritusoikeudet samoin kuin muillakin tietokoneen käyttäjillä. Käyttöoikeuksien tarkastelu onnistuu myös suoraan käyttöjärjestelmän käyttöliittymästä klikkaamalla kansiota tai tiedostoa ja valitsemalla yläpalkin “Arkisto” -valikosta “Näytä tietoja”. Avautuvassa ikkunassa oikeuksia ei näytetä “rwx” -muodossa vaan sanallisesti esimerkiksi “Luku ja kirjoitus”.

4.1.2 Tiedon salaaminen

Luvussa 4.1.1 käsitelty pääsynvalvonta menettää kuitenkin merkityksensä, jos asialla on taitava hakkeri tai koneen käyttöjärjestelmä asennetaan uudelleen (Paananen 2005, 398). Vähintään tärkeimmät kovalevyn sisältämät tiedot kannattaakin salata eli kryptata. Mac OS X käyttää salausratkaisuissaan pääasiallisesti symmetristä AES-algoritmia. Salauksessa selvätekstinen tieto muutetaan algoritmin sisältämällä matemaattisella kaavalla sekä salausavaimella salatekstiksi. Salausta purettaessa sama prosessi toistetaan, mutta toisin päin. Symmetrisessä salauksessa sekä salaus että salauksen purku tapahtuu käyttäen samaa salausavainta (kuvio 4). (Kissell 2009, 424-425.)



Kuvio 4. Salaus ja salauksen purku symmetrisellä salausmenetelmällä.

Mac OS X -käyttäjän tärkeimmät tiedostot sijaitsevat kotikansiossa. Jos käytössä on kannettava MacBook-kone ja kotikansio sisältää erityisen luottamuksellisia tietoja, kannattaa harkita kotikansion salaamista. Tämä onnistuu FileVault-ohjelmalla. FileVaultin ollessa päällä kotikansion tiedot kryptataan AES-algoritmilla ja käyttäjän sisäänkirjautumissalasanalla. Tiedostojen salaus ja salauksen purku tapahtuu “lennossa” tietoja käytettäessä. Kun käyttäjä on kirjautunut ulos tililtään, ulkopuolisten on mahdotonta päästä käsiksi kotikansion tietoihin tietämättä salasanaa.

Ennen FileVaultin käyttöönottoa käyttäjän kannattaa tehdä muutamia alkuvalmisteluja: koska tiedot ovat täysin turvassa vain silloin, kun käyttäjä on uloskirjautuneena, on tilin kirjautumisasetuksiin syytä tehdä muutoksia.

Järjestelmäasetuksien “Turvallisuus” -valikon kautta aktivoidaan “Estä automaattinen sisäänkirjautuminen” ja “Vaadi salasana heräämisen jälkeen tai näytönsäästäjän käynnistyttyä” (Kissell 2009, 446). Automaattinen uloskirjautuminen esimerkiksi 30 minuutin käyttämättömyyden jälkeen voidaan myös aktivoida, jos käyttäjä näkee sen tarpeelliseksi. Vielä ennen salauksen käyttöönottoa käyttöjärjestelmä vaatii ylläpitäjän asettamaan tietokoneelle pääsalasanan, jonka avulla voidaan nollata minkä tahansa käyttäjätilin sisäänkirjautumissalasana. Jos käyttäjä unohtaa sisäänkirjautumissalasanansa ja ylläpitäjä pääsalasanan FileVaultin ollessa päällä, käyttäjätilin kotikansion tiedot menetetään lopullisesti. Edellä mainitun tilanteen sekä tietojen korruptoitumisen varalta kotikansio kannattaa varmuuskopioida ennen FileVaultin käyttöönottoa. On myös huomattava, että FileVaultin ollessa käytössä Time Machine -ohjelman suorittamat automaattiset varmuuskopiot ajetaan ainoastaan käyttäjän ollessa uloskirjautuneena. Lisäksi yksittäisiä kotikansion sisältämiä tiedostoja ei voida palauttaa Time Machinen graafisen palautuskäyttöliittymän kautta.

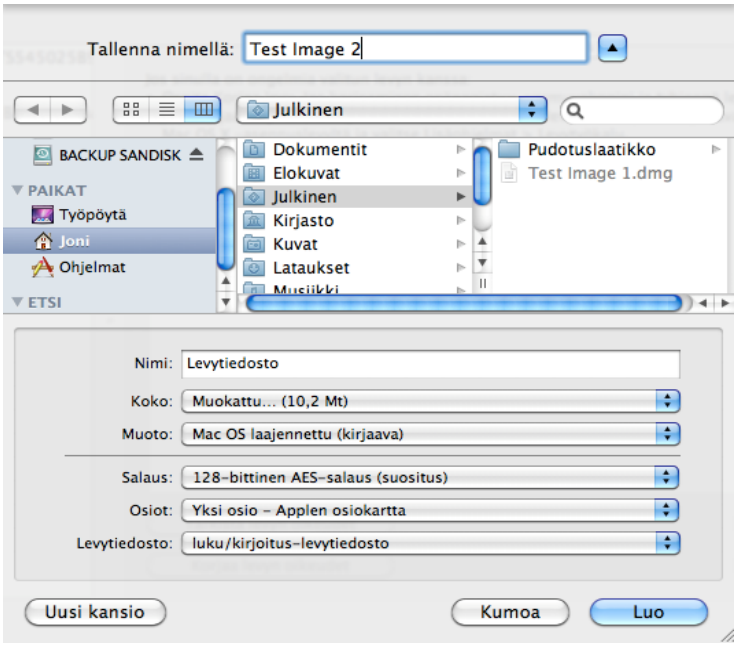
Alkuvalmisteluiden jälkeen FileVault voidaan kytkeä päälle järjestelmäasetuksien “Turvallisuus” -valikon kautta. Kotikansion kryptatun kopion luomisessa saattaa kulua paljonkin aikaa, jos kansio on suurikokoinen. Prosessin päätyttyä alkuperäinen kryptaamaton kotikansio poistetaan, jos käyttäjä päätti käyttää suojattua poistoa. Tämä asetus on syytä aina kytkeä päälle. FileVaultin suojaaman kotikansion tunnistaa kassakaappikuvakkeesta. Käyttöönoton jälkeen FileVaultin olemassaoloa ei juuri huomaa. Peruskäytössä automaattinen tietojen salaus ja salauksen purku eivät paljoa vaikuta tietokoneen suorituskykyyn. Hidastelua voi kuitenkin esiintyä, jos aletaan käsitellä yksittäisiä suurikokoisia tiedostoja. FileVaultin AES-salausalgoritmi on varmasti luotettava, mutta sisäänkirjautumissalasanan käyttö salausavaimena on ohjelman suurin haittapuoli. Erillisen ja monimutkaisen salausavaimen käyttömahdollisuus lisäisi huomattavasti käyttäjän mielenrauhaa. Pieni kiusa on myös salauksen huono yhteensopivuus sisäänrakennetun Time Machine -varmuuskopioinnin kanssa. Kolmannen osapuolen valmistamalla iBackup-

sovelluksella varmuuskopiointi saadaan kuitenkin hoidettua tehokkaasti myös FileVaultin ollessa päällä.

Kaikki käyttäjät eivät tarvitse kotikansion salausta, mutta yksittäisten tiedostojen ja kansioiden kryptaaminen saattaa joskus tulla ajankohtaiseksi. Esimerkiksi muistitikkujen arkaluontoinen sisältö kannattaa turvata. Mac OS X:n levytyökalu-ohjelmalla voidaan luoda erikokoisia kryptattuja levykuvia eli imageja.

Levytyökalu sijaitsee ohjelmahakemiston lisäohjelmat-kansiossa. Napsauttamalla “Uusi levytiedosto” päästään levytiedoston luonti-ikkunaan, jossa käyttäjä voi antaa levykuvan osiolle ja tiedostolle nimen sekä määrittää sen koon ja tallennuspaikan (kuva 3). Kätevin levytiedostotyyppi on niin kutsuttu harva levytiedosto, jonka koko kiintolevyllä kasvaa kohti määritettyä maksimia sitä mukaa kun tiedostoja lisätään (Kissell 2009, 434). Tiedostojärjestelmämuodoksi voidaan asettaa Applen HFS+:n lisäksi myös Windowsin tukema FAT. Salaukseksi voidaan määrittää joko 128-bittinen tai 256-bittinen AES. Salausavaimen voi käyttäjä päättää itse, toisin kuin FileVaultissa.

Tämän jälkeen levykuva luodaan ja sinne voidaan alkaa kopioida tiedostoja tai kansioita hiirellä raahaamalla. Levykuva tulee näkyviin sekä työpöydälle että Finderin vasemmalle laidalle. Kun halutut tiedostot on lisätty, käyttäjä poistaa levykuvan näkyvistä, jonka jälkeen tiedot ovat turvassa imagen sisällä salasanan takana. Mikäli image aiotaan säilyttää kovalevyllä, on muistettava, että imagen sisällä olevat tiedostot ovat vain kopioita, joten alkuperäiset salaamattomat tiedostot täytyy poistaa luottamuksellisuuden turvaamiseksi.



Kuva 3. Levykuvan luonti levytyökalulla.

4.2 Eheys

4.2.1 Haittaohjelmat ja virustorjunta

Tunnetuimpia eheyteen kohdistuvia uhkia ovat erilaiset haittaohjelmat. Saastuttaessaan tietokoneen kovalevyn haittaohjelma rikkoo samalla tietojen eheyden. Haittaohjelma on ylimääräinen lisä, jota kovalevyllä ei pitäisi olla. Haittaohjelmiksi luetaan kaikki ohjelmistot, jotka on suunniteltu tunkeutumaan tietokoneisiin ja sisään päästyään aiheuttamaan vahinkoa (Barker ym. 2010, 213). Haittaohjelma on siis kattotermi, johon kuuluvat muun muassa virukset, madot, troijalaiset ja takaovet. (Paananen 2005, 387, 410-411.)

Mac OS X -käyttöjärjestelmän tietoturvallisuutta uhkaavien haittaohjelmien määrä on tunnetusti pieni. Tarkkaa lukumäärää on vaikea arvioida, tosin iAntivirus-torjuntaohjelmisto listaa kotisivuillaan 116 Mac-haittaohjelmaa, joista osa toimii vain vanhoissa Mac-käyttöjärjestelmissä. Windows-ympäristöön suunnitellut haitalliset ohjelmat eivät toimi Mac-tietokoneissa. Saastuneet tiedostot voivat kuitenkin levitä Mac-ympäristöstä Windows-tietokoneisiin esimerkiksi sähköpostin tai ulkoisten tallennusvälineiden avulla. Windows-

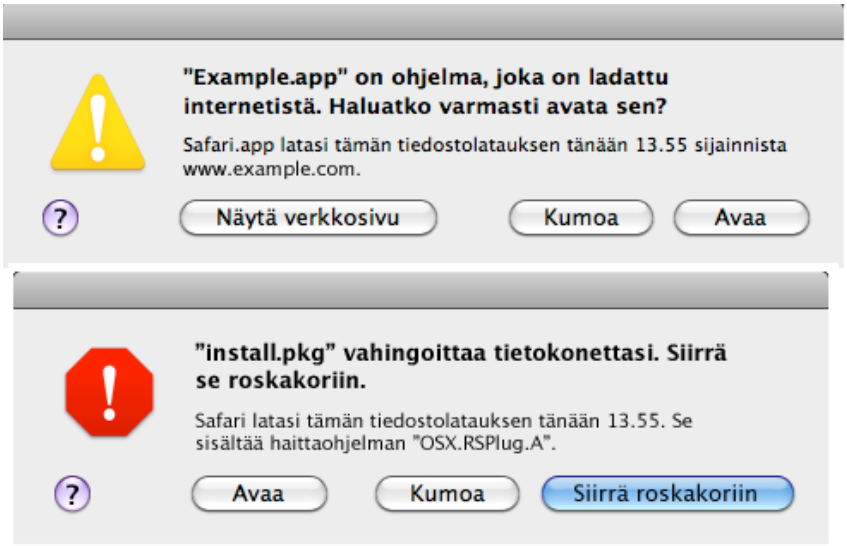
haittaohjelmien levitys Mac-koneesta ei kuitenkaan voi tapahtua automaattisesti, vaan syynä on yleensä käyttäjän huolimattomuus ja tietämättömyys.

Mac-tietokoneille suurimman varsinaisen haittaohjelmauhan muodostavat troijalaiset. Troijalaiset ovat ohjelmia, jotka näyttävät harmittomilta ja hyödyllisiltä, mutta todellisuudessa sisältävät haitallista koodia, joka vahingoittaa tietokonetta tavalla tai toisella (Kissell 2009, 465). Tähän mennessä merkittävin Mac-tietokoneille suunnattu haittaohjelma on MacDefender-troijalainen. MacDefender on valevirustorjuntaohjelma, joka yrittää huijata käyttäjän antamaan luottokorttitietonsa puhdistaakseen tietokoneen haittaohjelmista, joita ei todellisuudessa ole. Tekijät edesauttavat haittaohjelman leviämistä hakukoneoptimoinnilla saadakseen MacDefenderin sisältämät verkkosivut hakutuloksissa ylöspäin. Verkkosivulla vierailtaessa haittaohjelma imuroidaan kovalevylle automaattisesti, mutta ilman käyttäjän suorittamaa manuaalista asennusta ohjelma ei pysty tekemään vahinkoa. (The Mac Security Blog 2011.)

Paras tapa virustartuntojen ehkäisemiseksi on virustorjuntaohjelmiston asentaminen. Vaikka kyseisiä ohjelmistoja kutsutaan virustorjuntaohjelmiksi, pystyvät ne yleensä havaitsemaan ja tuhoamaan myös muunlaiset haittaohjelmat kuten madot, troijalaiset ja takaovet. Kaikilla haittaohjelmilla on tiettyjä yksilöllisiä piirteitä, joita torjuntaohjelma etsii kovalevyllä olevista tiedostoista ja sisääntulevasta verkkoliikenteestä. Nämä haittaohjelmien yksilölliset piirteet ja tarkat tiedot ovat tallennettuna torjuntaohjelmiston virustietokantaan, joka yleensä päivittyy automaattisesti. Uudet ja tietokannan ulkopuoliset haittaohjelmat voidaan havaita heuristisella tarkistusmenetelmällä. Heuristiikalla torjuntaohjelmisto pyrkii löytämään tietokoneesta haittaohjelmille tyypillisiä yleisiä käyttäytymismalleja, jotka todennäköisesti viittaavat tartunnan olemassaoloon. (Kissell 2009, 471-472.)

Mac OS X:ään sisältyy valmiina muutama alkeellinen virustorjuntaratkaisu, joiden avulla voidaan teoriassa estää monenlaisten haittaohjelmien suorittaminen. Kun käyttäjä lataa internetistä sovelluspaketteja, niihin lisätään automaattisesti tiettyjä metatietoja kuten lataussivuston osoite, latausajankohta

ja lataukseen käytetty ohjelma. Sovelluspakettia avattaessa ensimmäisen kerran kyseiset metatiedot näytetään varoitusikkunassa, jotta käyttäjä pystyy näkemään, onko sovellus ladattu huomaamatta (kuva 4). Automaattisesti ladattuja sovelluksia ei kannata avata, sillä ne voivat sisältää haittaohjelmia. Tunnetuimmat haittaohjelmat Mac OS X pystyy itse tunnistamaan suppeahkon virustietokannan avulla. Jos ladattu sovellus sisältää haittaohjelmakoodia, käyttäjää pyydetään siirtämään tiedosto roskakoriin (kuva 4). (Kissell 2009, 336-337.)



Kuva 4. Haittaohjelmatartuntoja ehkäiseviä varoitusikkunoita (Apple Inc. 2009).

Virustorjunnan laaja-alaiseen turvaamiseen vaaditaan ulkopuolisen valmistajan kehittämä ohjelmisto (taulukko 2). Mac-koneen virustorjuntaa hankittaessa kannattaa ottaa huomioon palvelun hinta sekä virustietokannan kattavuus. Windows-virukset kattava virustietokanta Mac-koneessa on erityisen tärkeä, jos siirretään tiedostoja PC-koneisiin. Lisäksi on varmistuttava, että ohjelmisto tukee käyttäjän koneeseen asennettua käyttöjärjestelmäversiota. Varsinkin uuden 10.7 Lion -version tuki on monissa ohjelmissa vielä puutteellinen.

Taulukko 2. Mac OS X:lle saatavilla olevia virustorjuntaohjelmistoja.

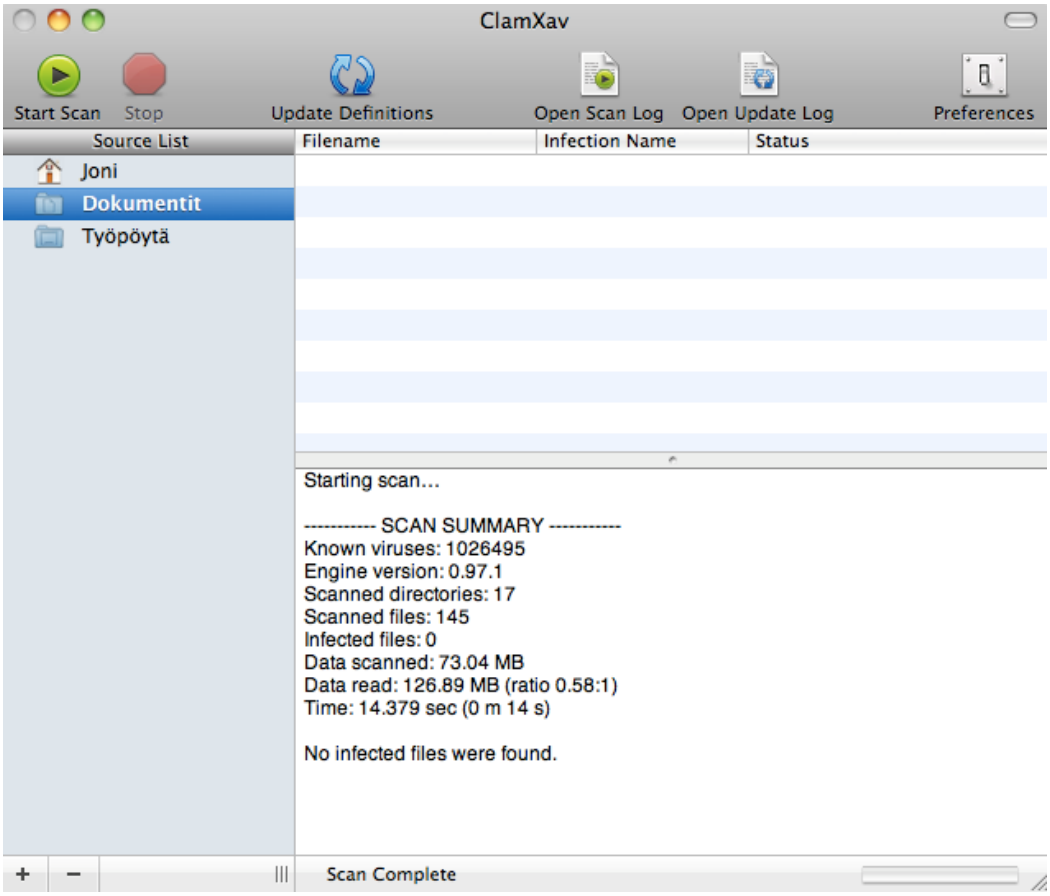
Tuote	Vuosihinta	Virustietokanta	Tuetut Mac OS X-versiot
avast! Mac Edition	42,78 €	Mac, PC	10.4 Tiger, 10.5 Leopard
ClamXav	Ilmainen	Mac, PC	10.4 Tiger →
F-Secure Antivirus for Mac	39,90 €	Mac, PC	10.5 Leopard, 10.6 Snow Leopard
iAntivirus	Ilmainen	Mac	10.5 Leopard, 10.6 Snow Leopard
Intego VirusBarrier X6	59,95 €	Mac, PC	10.5 Leopard →
Kaspersky Anti-Virus for Mac	59,95 €	Mac, PC	10.5 Leopard →
McAfee Virusscan for Mac	25,40 € (Ostettava väh. 3 lisenssiä)	Mac, PC	10.5 Leopard →
Norton AntiVirus for Mac	34,70 €	Mac, PC	10.4 Tiger, 10.5 Leopard, 10.6 Snow Leopard
Sophos Anti-Virus for Mac	Ilmainen	Mac, PC	10.4 Tiger →

Kotikäyttäjien keskuudessa yksi suosituimmista virustorjuntaohjelmistoista on vapaaseen lähdekoodiin perustuva ClamXav. ClamXavin käyttöliittymä on hyvin yksinkertainen sisältäen kaikki virustorjuntaohjelmistoille tyypilliset perustoiminnot (kuva 5). Virusten havaitsemiseen ja poistamiseen ohjelmisto tarjoaa kaksi erilaista tapaa: ensimmäinen tapa on perinteinen skannaus, jossa käyttäjä määrittää mitkä kovalevyn kohteet tarkistetaan. Yksittäisten tiedostojenkin tarkistus on mahdollista. Tietokoneen kovalevyn täystarkistusta ei suositella, sillä Mac OS X:n kansiorakenteesta johtuen skannaus voi joutua päättymättömään kehään (ClamXav 2011). Tarkistetut kohteet jäävät käyttöliittymän vasemmalla laidalla sijaitsevaan “Source Listiin”, joten tärkeitä kohteita ei tarvitse hakea joka kerta erikseen. Tarkistukset voidaan tietysti myös automatisoida aikatauluttamalla, aivan kuten virustietokannan päivityksetkin.

Toinen tapa on ClamXavin alaisuudessa toimivan aliohjelma ClamXav Sentryn käyttö. Sentry valvoo valittuja kovalevyn kansioita ja skannaa kaikki kansioon lisätyt uudet tiedostot. Liian ison kansiokokonaisuuden valvonta ei ole tarkoituksenmukaista, sillä tällöin koneen suorituskyky voi kärsiä. Sentry onkin parhaimmillaan silloin, kun se määrätään tarkkailemaan koneeseen liitettyjä ulkoisia tallennusvälineitä ja selaimen latauskansiota.

Loppujen lopuksi käyttäjä päättää itse, minkä tasoinen haittaohjelmaturva tarvitaan. Suppeita skannauksia ajamalla ClamXav ei juurikaan syö koneen

resursseja. Laaja-alaisempia tarkistuksia tehdessä suorituskyky laskee jonkin verran. Viikottaiset perusskannaukset ja ClamXav Sentryn käyttö riittävät varmasti turvaamaan Mac-koneen haittaohjelmilta.



Kuva 5. ClamXavin käyttöliittymä.

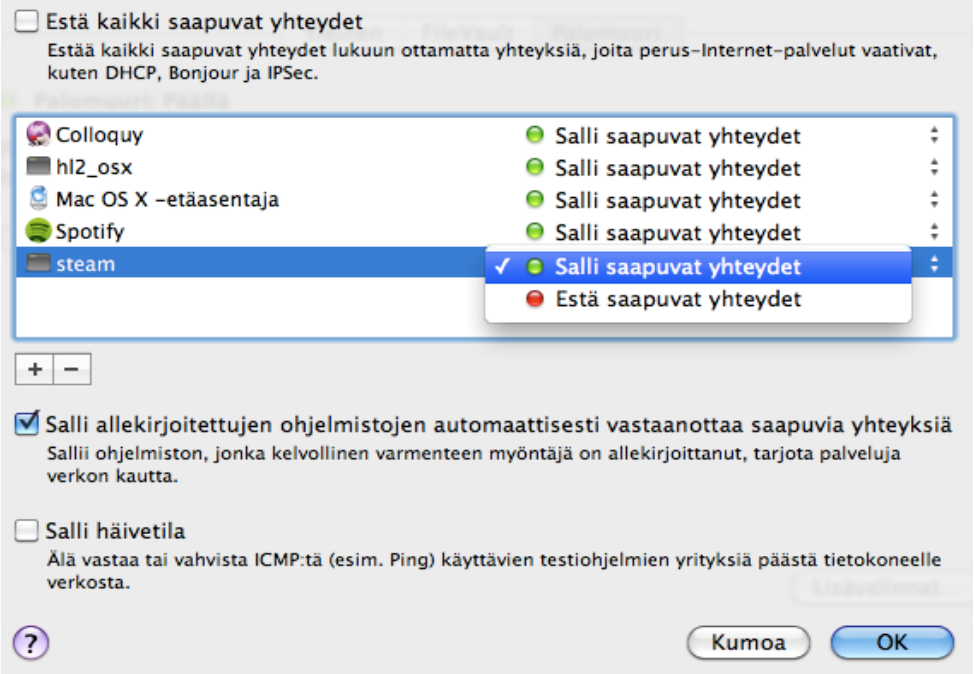
4.2.2 Palomuuri

Mac-tietokoneen eheyttä voidaan edelleen parantaa palomuurilla, joka valvoo ja tarvittaessa rajoittaa tietokoneen sisään- ja ulospäin suuntautuvaa verkkoliikennettä määrättyjen sääntöjen mukaan. Palomuurin avulla voidaan estää sellaiset haittaohjelmat, jotka yrittävät avata yhteyden verkon yli isäntäpalvelimeensa. Lisäksi palomuuri on tehokas keino tietomurtojen ehkäisemisessä. Murtautuessaan tietojärjestelmään hakkeri rikkoo välittömästi tietojen eheyden. (Paananen 2005, 388, 403-405.) Kokonaisvaltaisen tietoturvan saavuttamiseksi palomuuri on välttämätön apuväline, sillä laitteisto- tai ohjelmistopohjainen palomuuri pystyy torjumaan kaikkiin CIA-triadin

tukipilareihin kohdistuvia uhkia. Eheyden lisäksi tietojärjestelmän tietoihin käsiksi päässyt hakkeri vaarantaa tietojen luottamuksellisuuden. Palomuurin avulla voidaan myös estää tietojen saatavuutta uhkaavat palvelunestohyökkäykset.

Mac OS X sisältää kaksi palomuuriratkaisua, jotka ovat toimintatavaltaan ja käytettävyydeltään toistensa vastakohtia. Järjestelmäasetuksien “Turvallisuus” -valikon kautta hallittava sovelluskohtainen palomuuri on helppokäyttöinen, mutta ominaisuuksiltaan niukka ratkaisu (kuva 6). OS X:n sovelluskohtainen palomuuri valvoo ainoastaan sovelluksien sisäänpäin tulevaa verkkoliikennettä sekä sallii ja rajoittaa sitä käyttäjän kokoaman listan pohjalta. Palomuurin ollessa päällä oletusasetuksilla palomuuri hyväksyy automaattisesti vain sertifikaatilla allekirjoitetut luotettujen sovellusten yhteydet. Luotettuja sovelluksia ovat esimerkiksi kaikki Applen valmistamat ohjelmat (Kissell 2009, 553). Luotettujen sovellusten automaattinen salliminen voidaan tarvittaessa kytkeä pois päältä. Kun allekirjoittamaton sovellus muodostaa yhteyden koneelle ensimmäisen kerran, kysytään käyttäjältä sallitaanko kyseinen yhteys. Riippuen käyttäjän vastauksesta sovellus lisätään palomuurin listalle joko sallittuna tai estettynä. Sovelluksia voidaan tietysti lisätä listalle myös manuaalisesti palomuurin hallintaikkunan kautta.

Korkeatasoisimman tietoturvan saavuttamiseksi palomuuri voidaan ohjeistaa estämään kaikki saapuvat yhteydet. Tämän asetuksen ollessa päällä vain tärkeimmät internetpalvelut kuten IP-osoitteiden jakamisesta vastaava DHCP-protokolla jäävät päällekytketyiksi. Samalla aktivoidaan niin kutsuttu häivetila (Stealth mode), joka tekee tietokoneen löytämisen verkosta vaikeammaksi. Häivetilan käyttö ei vaikuta sovellusten sisäänpäin suuntautuvan verkkoliikenteen rajoittamiseen tai sallimiseen, joten sitä voidaan käyttää myös “Estä kaikki saapuvat yhteydet” -asetuksen ollessa pois päältä.



Kuva 6. Sovelluskohtaisen palomuurin hallintaikkuna.

Sovelluskohtaisen palomuurin suurimpia haittapuolia on kykenemättömyys valvoa tietokoneelta ulospäin suuntautuvaa liikennettä. Lisäksi palomuuria ei voida ohjelmoida kuuntelemaan verkkoliikennettä porttikohtaisesti. Ratkaisut näihin puutteisiin tuo sisäänrakennettu Unix-perinteisiin nojaava IPFW-palomuuri, joka tosin on oletuksena kytketty pois päältä (Kissell 2009, 557). IPFW-palomuuria hallitaan komentotasolta erilaisia käskyjä antamalla, mikä luonnollisesti monimutkaistaa palomuurin konfigurointia. Käytön helpottamiseksi internetistä on onneksi saatavilla IPFW-palomuuriin liitettäviä graafisia käyttöliittymiä. Näitä ovat esimerkiksi WaterRoof ja NoobProof.

4.3 Saatavuus

4.3.1 Varmuuskopiointi

Saatavuuteen kohdistuvan uhan toteutuessa tieto voi tuhoutua kokonaan tai pääsy siihen estyä joko hetkellisesti tai lopullisesti. Vakavampia uhkia Mac OS X-käyttöjärjestelmän sisältämien tietojen saatavuudelle ovat varkaudet ja laiteviat. Varkauksien mahdollisuus on Mac-koneilla erityisen suuri johtuen laitteiden arvosta ja trendikkyydestä. Tietoturva-asioissa ennaltaehkäisevät

suojatoimenpiteet ovat aina parhaita vaihtoehtoja. Täten varkauksista johtuvien tietomenetyksien estämiseksi laitteen omistajan järjenkäyttö on avainasemassa esimerkiksi säilytyspaikkoja ajateltaessa. Laitevikoja voidaan ehkäistä panostamalla laadukkaisiin tuotteisiin ja käytön aikana seuraamalla niiden toimintaa (Valtiovarainministeriö 2003, 46). Tässä opinnäytetyössä ei kuitenkaan paneuduta tämän enempää fyysisen turvallisuuden ja laitteistoturvallisuuden tarjoamiin suojamenetelmiin.

Yksinään ennaltaehkäisevät toimenpiteet eivät riitä tietojen saatavuuden turvaamiseen. Uhan toteutuessa on otettava käyttöön korjaavat menetelmät, joista käytetyin on varmuuskopiointi. Yksinkertaisuudessaan varmuuskopiointi tarkoittaa tietojen kahdentamista esimerkiksi ulkoiselle kovalevylle, muistitikulle tai varmuuskopiointipalvelimelle. Tietojen kadotessa tai tuhoutuessa ne voidaan helposti palauttaa varmuuskopioiden tallennuspaikasta, minkä jälkeen työskentelyä voidaan jatkaa normaalisti. Varmuuskopioinnista ei kuitenkaan ole merkittävästi hyötyä, jos sitä ei tehdä säännöllisesti (Paananen 2005, 398). Lisäksi on huolehdittava tallennuspaikan riittävästä kapasiteetista, jotta levytila ei lopu kesken varmuuskopiointiprosessin.

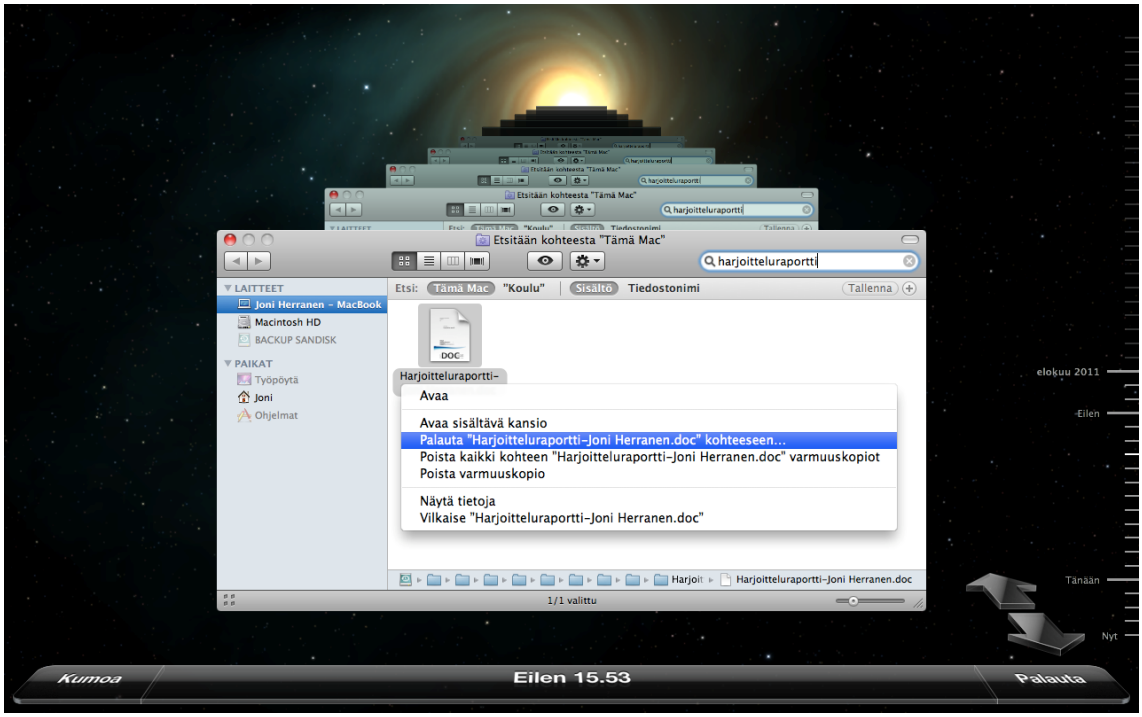
Mac OS X:ssä kotikäyttäjän varmuuskopiointi on helppo toteuttaa Time Machine -ohjelmalla. Jos käytössä on Applen Time Capsule -verkkokovalevy, automaattisen varmuuskopioinnin valmisteluun ei tarvita kuin muutama napsautus. Time Machinen käyttö on tietysti mahdollista myös muiden valmistajien ulkoisilla kovalevyillä ja USB-tikuilla. Ulkopuolisten valmistajien tallennusvälineet joudutaan kuitenkin alustamaan Mac OS X:n käyttämään HFS+ -tiedostojärjestelmämuotoon ennen käyttöönottoa. Varmuuskopiointi voidaan ottaa käyttöön ohjelmakansiossa sijaitsevan Time Machine -hallintaikkunan kautta (kuva 7). Hallintaikkunassa käyttäjän on määritettävä varmuuskopioiden tallennuspaikka sekä tarvittaessa kansiot, joita ei varmuuskopioida.

Kuva 7. Time Machinen hallintaikkuna.

Alkuvalmisteluiden jälkeen ohjelma suorittaa kertaalleen kaikkien haluttujen kovalevyn kohteiden täysvarmuuskopioinnin ja sitten ainoastaan muuttuneiden tiedostojen varmuuskopioinnin (Inkrementaalinen varmuuskopiointi) kerran tunnissa. Time Machine säilyttää tunnin välein tehtävät kopiot kuluneelta 24 tunnilta, päivän ensimmäiset kopiot kuluneelta kuukaudelta sekä viikoittain tehtävät kopiot kaikilta menneiltä kuukausilta. Kun levy täyttyy, uusimmat varmuuskopiot kirjoitetaan vanhimpien päälle. Varmuuskopioinnin tiheyttä ei voida muuttaa ilman kolmannen osapuolen valmistamaa sovellusta. Esimerkiksi TimeMachineScheduler -sovelluksella tiheyttä voidaan muuttaa tunnista 12 tuntiin.

Tiedostojen ja kansioiden palautus tapahtuu erillisellä käyttöliittymällä, johon pääsee napsauttamalla Time Machine -kuvaketta dockissa tai valikkorivillä (kuva 8). Palautuskäyttöliittymä toimii aikakoneena näyttäen tietokoneen kovalevyn sisällön tiettynä ajanhetkenä varmuuskopioitujen tietojen osalta. Näytön oikeassa reunassa sijaitsevien painikkeiden avulla käyttäjä pystyy liikkumaan ajassa taaksepäin ja eteenpäin. Haettavan tiedoston tai kansion

sijaintia ei tarvitse muistaa, sillä ikkunan oikeassa yläkulmassa olevaa hakukenttää käyttämällä tiedot on helppo löytää.



Kuva 8. Tiedoston palautus varmuuskopioista.

Time Machine on suunniteltu kotikäyttäjiä silmällä pitäen. Yksinkertaisen alkuvalmistelun jälkeen ohjelma toimii taustalla automaattisesti, eikä sen olemassaoloa juuri huomaa. Esimerkiksi varmuuskopioitaessa pelkästään omaa kotikansiota on kerran tunnissa suoritettava varmuuskopiointiprosessi nopea, eikä se syö koneen resursseja merkittävästi. Ohjelman yksinkertaisuus ja helppokäyttöisyys johtuu osin edistyneempien varmuuskopiointiominaisuuksien puutteesta. Yrityksien varmuuskopioinnin toteuttamiseen Time Machine ei sovellu riittävän hyvin. Yksi suurimmista haittapuolista on kiinteä varmuuskopiointitiheys.

4.3.2 Salasanahallinta

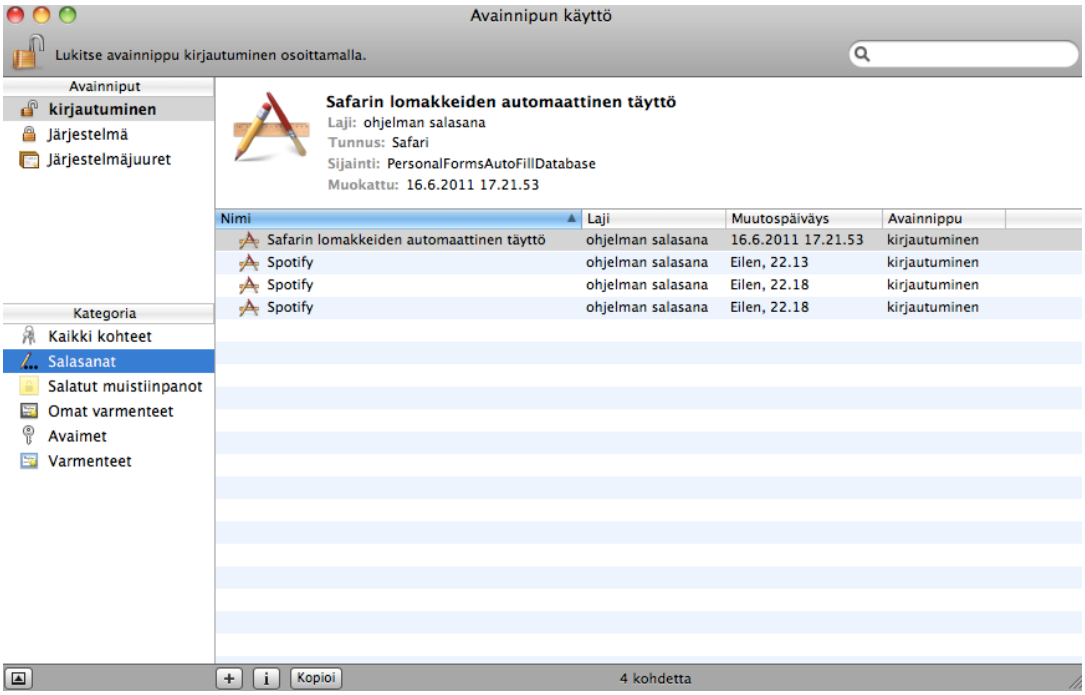
Saatavuuden ja luottamuksellisuuden tasapainottaminen voi joskus olla vaikeaa. Kotikäyttäjille konkreettisin esimerkki tästä ovat salasanat. Käyttäjillä on usein lukuisia salasanalla suojattuja kohteita, kuten tietokoneen käyttäjätili, sähköposti ja satunnaiset kirjautumista vaativat verkkopalvelut. Saman salasanan käyttöä kaikissa kohteissa ei suositella, sillä tällöin turvataan tehokkaasti vain saatavuus, mutta ei luottamuksellisuutta. Toisaalta kaikkien salasanojen ollessa uniikkeja luottamuksellisuus paranee, mutta saatavuus saattaa vaarantua, koska kaikkia salasanoja on vaikea muistaa. Tilannetta voidaan tasapainottaa käyttämällä salasananhallintaohjelmaa, joka toimii eräänlaisena salasanojen säilöntäpaikkana.

Mac OS X helpottaa salasanojen hallinnointia niin kutsuttujen avainnippujen (Keychain) avulla (kuva 9). Niihin voidaan tallentaa muun muassa salasanoja, sertifikaatteja, salausavaimia, lomaketietoja ja muistiinpanoja. Itse avainnippu kryptataan ja suojataan salasanalla, jonka avulla päästään käsiksi nipussa oleviin salasanoihin. Tämä tarkoittaa, että useiden salasanojen muistamisen sijasta käyttäjän tarvitsee muistaa ainoastaan avainnipun salasana kirjautuessaan kohteeseen, jonka salasanan avainnippu sisältää. Avainnipun pääsalasanan monimutkaisuuteen kannattaa kiinnittää erityistä huomiota, sillä nipun sisältämät salasanat ovat käyttöönoton jälkeen yhtä heikkoja tai vahvoja kuin pääsalasana. Toisin sanoen, jos pahantekijä jollain tavalla onnistuisi hankkimaan avainnipun pääsalasanan, olisi hänellä tällöin pääsy kaikkiin avainnipun sisältämiin salasanoihin.

Oletusasetuksilla käytettäessä avainnippu on melko turvaton. Oletuksena käyttäjän haluamat salasanat tallennetaan kirjautumisavainnippuun, joka tarkoittaa, että tietokoneelle sisäänkirjautumisen jälkeen kyseiset salasanat syötetään kysyttäessä automaattisesti. Tällöin avainnipun sanotaan olevan auki. Käyttäjän kannattaakin "Lisäohjelmat" -kansiossa sijaitsevan avainnippujen hallintaikkunan kautta luoda erillinen monimutkaisella salasanalla varustettu avainnippu ja asettaa se oletukseksi. Turvallisuuden parantamiseksi asetuksista kytketään päälle "Lukitse 5 minuutin käyttämättömyyden jälkeen" ja "Lukitse

nukkuessa", sillä avainnipun ollessa auki kaikkiin nipun sisältämien salasanojen kohteisiin on vapaa pääsy.

Avainnippujen käyttö ei ole pakollista, mutta oikein konfiguroituina ne parantavat kohteiden saatavuutta luottamuksellisuutta vaarantamatta. Teho perustuu siihen, että kaikki käyttäjän salasanat voidaan pitää monimutkaisina ja erilaisina, koska ne ovat helposti saatavissa yhdellä pääsalasanalla. Avainnippujen integrointi jokapäiväiseen käyttöön on huomaamatonta, tosin internetiä käytettäessä niput toimivat parhaiten Applen Safari-selaimella.



Kuva 9. Avainnippujen hallintaikkuna.

5 TIETOTURVAVINKKEJÄ MAC-KÄYTTÄJILLE

Mac OS X on tunnetusti turvallinen käyttöjärjestelmä jo tehdasasetuksilla käytettäessä, mutta muutamilla nopeilla toimenpiteillä Mac-tietokoneen tietoturvatasoa voidaan nostaa vieläkin korkeammaksi. Osaa seuraavista vinkeistä on sivuttu jo edellisessä kappaleessa, mutta eri näkökulmasta. Käyttäjien vaatimukset kotikoneen tietoturvalle vaihtelevat, mutta jotkin tietoturvakäytänteet nousevat yleisesti tärkeämmiksi kuin toiset.

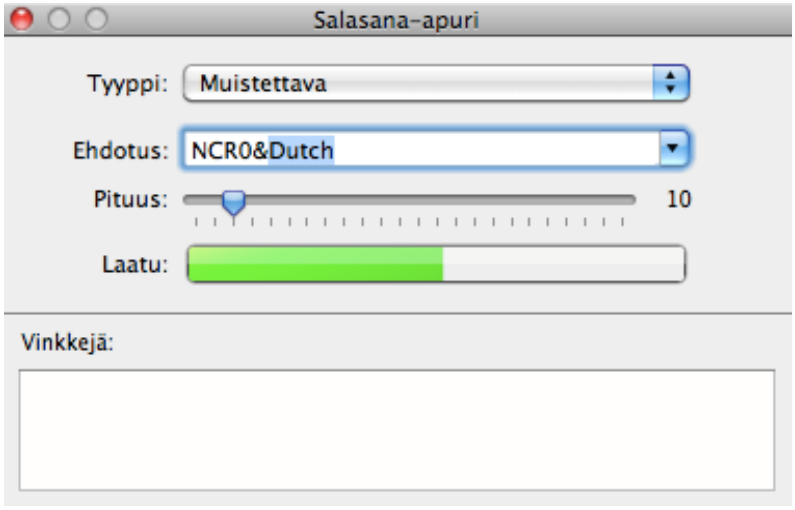
Käyttäjätileillä on suuri merkitys tietojen luottamuksellisuuden turvaamisessa. On itsestään selvää, että kaikki tilit tulisi suojata salasanalla, mutta erilaisten tilityyppien käyttöön on myös kiinnitettävä huomiota. Mac OS X:n asennusvaiheessa luodaan yksi ylläpitäjätili, jota monet jäävät käyttämään normaalissa tietokoneenkäytössä. Tämä ei kuitenkaan ole suositeltavaa, sillä esimerkiksi Mac-haittaohjelmat vaativat yleensä ylläpito-oikeudet asentuakseen. Lisäksi pahantekijä voi ylläpitäjätilin kaappaamalla omaksua root-käyttäjän oikeudet ja siten saada aikaan paljon vahinkoa. Käyttäjän kannattaakin luoda jokapäiväiseen käyttöön normaali käyttäjätili ja käyttää ylläpitäjätiliä vain ylläpitotehtävien suorittamiseen kuten ohjelmien asentamiseen ja järjestelmäasetuksien muuttamiseen.

Internetin keskustelupalstoilla käydään paljon keskustelua siitä, onko virustorjuntaohjelman asentaminen Mac-koneeseen tarpeellista. Mac-haittaohjelmien määrä on tunnetusti pieni ja käyttöjärjestelmän rakenteesta johtuen viruksien on vaikea tehdä tuhoa. Windows-haittaohjelmatkaan eivät toimi Mac-koneissa. Edellä mainitut näkökannat ovat kuitenkin subjektiivisia ja vain kolikon toinen puoli. On muistettava, että virustorjuntaohjelma suojaa yksittäisen koneen lisäksi myös muita käyttäjiä, sillä Windows-virusten leviäminen Mac-koneesta ei ole mahdotonta, jos käyttäjä on huolimaton. Tästä voidaan päätellä, että paljon sähköpostin liitetiedostoja lähettäville käyttäjille virustorjuntaohjelman asentaminen on suositeltavaa. Tällöin on pidettävä huoli, että ohjelma sisältää sekä Mac- että Windows-haittaohjelmat tunnistavan virustietokannan.

Mac OS X:n kahdesta palomuuriratkaisusta on syytä käyttää ainakin sovelluskohtaista palomuuria. Otettaessa käyttöön uutta Mac-konetta, on muistettava, että kumpikaan palomuureista ei ole oletuksena kytkettynä päälle. Palomuurien yhteiskäyttö ei aiheuta ongelmia, sillä ne toimivat eri toimintaperiaatteilla.

Loput vinkit ovat käyttöjärjestelmäriippumattomia ja liittyvät tietokoneen jokapäiväiseen käyttöön. On päivänselvää, että täysin tietoturva-aukotonta käyttöjärjestelmää ei ole, eikä tule olemaankaan. Kun uusia aukkoja löytyy, käyttöjärjestelmien kehittäjät pyrkivät parhaansa mukaan julkaisemaan tietoturva-aukot tukkivia korjauspäivityksiä. Myös Mac OS X-käyttäjän tulisi aina ladata ja asentaa uusimmat päivitykset heti kun ne tulevat saataville. Tämä tapahtuu napsauttamalla omenalogoa ruudun vasemmasta ylälaidasta ja valitsemalla “Ohjelmiston päivitys”.

Kaikkein suurinta tietoturva-aukkoa ei kuitenkaan pysty korjaamaan päivityksillä, sillä uhka on käyttäjä itse. Käyttäjän huolimattomuus ja tietämättömyys tietoturva-asioissa luovat monenlaisia riskejä. Tyypillisiä virheitä ovat varomaton sähköpostin liitetiedostojen availu, epäilyttävillä sivustoilla surffailu ja huonot salasanat. Hyvien salasanojen luomiseen Mac OS X tarjoaa näppärän salasana-apurin (kuva 10). Salasana-apurin tunnistaa avainkuvakkeesta, joka esiintyy aina uutta salasanaa luotaessa käyttöjärjestelmän sisällä. Apurin avulla voidaan generoida halutun pituisia ja muotoisia salasanoja sekä testata oman salasanan vahvuus. Sovellusta voidaan pyytää luomaan esimerkiksi satunnaisia kirjaimia ja numeroita sisältävä salasana tai helpommin muistettava sanoja ja numeroita sisältävä salasana. Salasanan vahvuus näkyy ikkunan alalaidassa.



Kuva 10. Salasana-apuri.

6 POHDINTA

Tämän opinnäytetyön tarkoituksena oli tutkia Mac OS X:n sisäänrakennettuja tietoturvaratkaisuja CIA-triadin toteuttajina. Aiheeseen liittyvän suomenkielisen aineiston ollessa suppeaa oli työn tavoitteena saada aikaan riittävän kattava katsaus Mac OS X:n tietoturvaan. Aihetta lähestyttiin uuden Mac-käyttäjän näkökulmasta, joten käyttöjärjestelmän teknisten ominaisuuksien läpikäynti opinnäytetyön alkuvaiheessa on perusteltua. Mac OS X:n tietoturvaa tarkasteltaessa on tärkeää ymmärtää käyttöjärjestelmän Unix-pohjaisuus, sillä osa OS X:n tietoturvaratkaisuista periytyy suoraan "esi-isältään".

Applen ja Macintoshin tuotefilosofian mukaisesti OS X:n tietoturvasovellukset on suunniteltu käyttäjäystävällisiksi ja helppokäyttöisiksi. Suurimmalle osalle tietokoneenkäyttäjistä ongelmaksi ei muodostu tietoturvaratkaisujen käyttäminen, vaan pikemminkin niiden löytäminen. Ratkaisuja läpikäytäessä pääpaino olikin enemmän sovelluksien esilletuonnissa kuin käytön opastuksessa. Sovelluksia suunnitellessaan Apple on selkeästi tehnyt kompromisseja helppokäyttöisyyden ja monipuolisten ominaisuuksien välillä. Tietoturvaratkaisujen helppokäyttöisyys johtuu siis osin edistyneempien ominaisuuksien puutteesta. Tästä johtuen Mac OS X:n sisäänrakennetut tietoturvaratkaisut eivät sovellu erityisen hyvin yrityskäyttöön, mutta onneksi internetissä on tarjolla lukuisia kolmannen osapuolen kehittämiä monipuolisempia tietoturvaohjelmistoja.

Edelliseen lauseeseen peilaten ja tulevia tutkimuksia ideoitaessa hyvä aihe voisi olla Mac OS X yrityksen tietoturvan kannalta. Lisäksi heinäkuussa 2011 julkaistu "10.7 Lion" -käyttöjärjestelmäversio toi mukanaan joitakin tietoturvauudistuksia, joiden tarkastelu on paikallaan käyttöjärjestelmän yleistyessä. Erityisen mielenkiintoisia uudistuksia ovat FileVault 2-salaus sekä iCloud-pilvipalvelu ja sen vaikutukset kotikäyttäjän tietoturvaan.

Opinnäytetyöprosessi on ollut erittäin opettavainen polku kuljettavaksi, sillä itselläni ei ollut paljoa aikaisempaa Mac-kokemusta. Toivon ja uskon, että

opinnäytteestä on hyötyä muillekin. Mac-koneiden suosion kasvaessa ja uhkien lisääntyessä Mac-käyttäjien on oltava entistä valveutuneempia tietoturvan suhteen. Välinpitämätön asenne tietoturva-asioissa saattaa osoittautua kalliiksi tulevaisuudessa.

LÄHTEET

Apple Inc. 2009. Tietoja tiedostokaranteenista Mac OS X 10.5:ssä ja 10.6:ssa. Viitattu 17.8.2011 http://support.apple.com/kb/HT3662?viewlocale=fi_FI.

Apple Inc. 2011. Introduction to Apple Human Interface Guidelines. Viitattu 4.7.2011 http://developer.apple.com/library/mac/#documentation/UserExperience/Conceptual/AppleHIGuidelines/XHIGIntro/XHIGIntro.html.

Barker, W.; Edge, C.; Hunter, B. & Sullivan, G. 2010. Enterprise Mac Security: Mac OS X Snow Leopard. New York: Apress.

Brown, E. 2000. How to Think Like the World's Greatest High-Tech Titans. Blacklich: McGraw-Hill Trade.

Chapple, E.; Stewart, M. & Tittel, JM. 2008. CISSP: Certified Information Systems Security Professional Study Guide. 4. painos. Indianapolis: Wiley.

ClamXav 2011. ClamXav FAQs. Viitattu 23.8.2011 http://www.clamxav.com/faq.php#Q7.

Clancy, T.; Costa-Woods, E.; Gottlieb, W.; Heyman, D.; Litt, S. & Zuckerman, S. 2008. Mac OS X Leopard Bible. Indianapolis: Wiley.

Information Systems Security Working Group 2011. Security?. Viitattu 18.7.2011 http://www.isswg.org.uk/cia.php.

Kissell, J. 2009. Mac Security Bible. Indianapolis: Wiley.

The Mac Security Blog 2011. Intego Security Memo - MAC Defender Fake Antivirus Program Targets Mac Users. Viitattu 26.7.2011 http://blog.intego.com/2011/05/02/intego-security-memo-macdefender-fake-antivirus/.

McCormack, D. & Trent, M. 2010. Beginning Mac OS X Snow Leopard Programming. Hoboken: Wrox.

Merriam Webster 2011. Learner's Dictionary- Plug and Play. Viitattu 5.7.2011 http://www.learnersdictionary.com/search/plug%20and%20play.

Mitchell, D. 2007. Apple Cult Becoming a Religion. Viitattu 22.6.2011 http://www.nytimes.com/2007/03/24/technology/24online.html.

Paananen, J. 2005. Tietotekniikan peruskirja. 1. painos. Jyväskylä: Docendo.

Reuters 2011. Apple Inc (AAPL.O) Company Profile. Viitattu 22.6.2011 http://www.reuters.com/finance/stocks/companyProfile?symbol=AAPL.O.

Rigby, B. 2010. Apple overtakes Microsoft as biggest tech company. Viitattu 22.6.2011 http://www.reuters.com/article/2010/05/26/us-apple-stock-idUSTRE64P5PE20100526.

StatOwl.com 2011. Operating System Version Usage. Viitattu 27.6.2011 http://www.statowl.com/operating_system_market_share_by_os_version.php?limit%5B%5D=windows&limit%5B%5D=mac&limit%5B%5D=linux.

Valtiovarainministeriö 2003. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. Viitattu 14.7.2011
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf.