LAUREA

Mistä tiedän onko virtuaalikoneeni varastettu?

Arte, Eero

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Mistä tiedän onko virtuaalikoneeni varastettu?

Eero Arte
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2008

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittely
Yrityksen Tietoverkot

Eero Arte

Mistä tiedän onko virtuaalikoneeni varastettu?

Vuosi 2008 Sivumäärä 32

Tutkimukseni aiheena on tunnetun virtualisointisovelluksen, VMware Player –nimisen sovelluksen ominaisuus, jossa sovelluksen sulkeminen ei sammuta virtualisoitua käyttöjärjestelmää vaan sulkee sen ns. nukkumistilaan. Virtualisointisovellus tarjoaa mahdollisuuden ajaa teoriassa mitä tahansa käyttöjärjestelmää sovelluksen sisällä, ja sovellus toimii teoriassa missä tahansa Windows-pohjaisessa tietokoneessa. Virtualisointisovellus tarjoaa geneeriset laiteajurit, jotka tarjoavat virtualisoidulle käyttöjärjestelmälle mahdollisuuden toimia missä tahansa tietokoneessa.

Ongelmaksi muodostuu käyttöjärjestelmän helppo kopioitavuus tallennusmedialta sekä sovelluksen avaaminen nukkumatilasta. Nukkumatilasta sovelluksen avaaminen ei autentikoi käyttäjää uudelleen. Autentikointia ei tapahdu käyttöjärjestelmään eikä mahdollisiin VPN-yhteyksiin, koska virtualisoitu käyttöjärjestelmä avautuu juuri siitä tilasta, josta virtualisointisovellus on suljettu. Jos virtualisoitu käyttöjärjestelmä kopioidaan tallennusmedialta nukkumatilasta, avautuu kopio käyttöjärjestelmästä myös ilman autentikointia.

Tutkimuskysymys tutkimukselle on ”mistä tiedän onko virtuaalikoneeni varastettu?” Jos tiedosto kopioidaan nukkumatilassa, on kopion tekijällä pääsy yrityksen tietoverkkoon ja tietojärjestelmiin ilman autentikointia. Sovelluksen ominaisuudesta tulee tietoturvariski.

Kryptaus perinteisenä suojausmenetelmänä ei välttämättä ole paras mahdollinen vaihtoehto suojata luottamuksellista tietoa, tässä tapauksessa virtualisoitua työasemaa. Organisaatiot harkitsevat tietoturvapolitiikallaan riittävää suojausmetodia ja tutkivat eri työvälineiden käytettävyyttä. Organisaatio kartoittaa, voiko edes sen tietoturvapolitiikan mukaan suojaamalla saavuttaa tarvittavaa suojaustasoa.

Olen opinnäytetyössäni keskittynyt modernimpaan DRM-suojausmenetelmien tutkimiseen virtualisoidun työaseman suojaamiseksi. DRM-suojaus keskittyy operaatioihin liittyviin rajoituksiin, kun kryptausteknologiat suojausmetodeina keskittyvät lähtökohtaisesti pelkästään tiedon avaamisen estämiseksi. DRM-suojauksella voidaan estää esimerkiksi dokumenttien tulostaminen tai tiedoston kopioiminen muistitikulta.

Lopputuloksena jää kysymykseksi yrityksen tietoturvapolitiikka. Yksityshenkilölle jo perinteinen kryptausmenetelmä voi tarjota riittävän suojan virtualisoidulle työasemalle. Yritysmaailmassa vastaus ei ole niin yksiselitteinen. Yrityksen tietoturvapolitiikka sanelee, tarjoaako mikään suojausmenetelmä riittävän suojauksen tietoturvapolitiikan puitteissa. Organisaatio voi katsoa, että virtualisoitu työasema on liian riskialtis väärinkäytöksille ja luottamuksellisen tiedon käsittelylle.

Asiasanat: Virtualisointi, DRM

Laurea University of Applied Sciences
Laurea Leppävaara
Information Technology Programme
Networks

Abstract

Eero Arte

How do I know if my virtual PC is stolen?

Year 2008 Pages 32

The thesis is based on a feature of a virtualization software called Player, which is a free downloadable software made available by VMware Inc. The virtualization software enables the virtualized operating system to work in any windows based personal computer through a set of generic drivers embedded in the virtualization software.

The Player software has a feature, where the user shuts down the virtualization software. The virtualized operating system does not shut down but puts it to a hibernation state. The problem is the feature itself. If the virtualized operating system has authentication to a company local area network through basic windows logon authentication and VPN-authentication, opening the operating system from the hibernation state does not authenticate the user. The authentication has already happened on the first logon using the virtualized operating system.

The virtualized operating system can be stored and used from a simple flash-drive. The actual operating system is only one image file stored on the flash-drive. Copying the image-file while the operating system is in a hibernation state is a serious problem, because the copied file does not authenticate the user if closed in the right state as explained in the paragraph above.

The thesis deals with finding the right solution to protect the copying and operating of confidential information, here a virtualized operating system, through using digital rights management - based technologies. Where normal encryption is based on accessing information, the DRM-solutions is based on restricting the operations within the information. For example, DRM-protected documents can deny the printing of the document.

Through DRM-based protection, the virtualized operating system can be protected from copying the image file by embedding a piece of code to the file itself. The code states, that the image file can only be run from a particular flash-drive based on a device-id embedded in the flash-drive.

Organizations themselves analyze their security solutions through a correct method of information security safeguards. Like where the problem of shutting down a virtualized operating system to a hibernation state violates the organizations security policy even if the operating system is encrypted or protected with a DRM-solution. The organization itself analyzes if the best possible solution offers sufficient security for using a virtualized operating system on a small flash-drive.

Key words: Virtualization, DRM

Sisällys

1 Johdanto

Tutkin opinnäytetyössäni ongelmaa, joka vastaa kysymykseen: ”Onko virtualisoitutietokoneeni varastettu?”. Perinteisten työvälineiden, kuten kannettavan tietokoneen osalta kysymys on selkeä. Oman kannettavan tietokoneen huomaa varastetuksi itsestään selvien seikkojen kautta. Kannettava tietokone on fyysisesti poissa. Virtuaaliratkaisuissa varastamista tai väärinkäyttöä ei välttämättä heti huomaa. Virtualisoitu työasema on käytännössä yksi tiedosto esimerkiksi muistitikulla tai ulkoisella kiintolevyllä. Mistä tiedän onko tiedostoani kopioitu? Miten kopioimisen voisi estää tai ainakin tehdä siitä hyödyttömän?

Olen tutkinut ongelmaa käyttäen VMware Player -nimistä tuotetta, jolla voidaan ajaa virtuaalisesti käyttöjärjestelmiä. Olen myös luonut VPN-ratkaisulla suojatun yhteyden suljettuun verkkoon ja testannut virtuaalikoneen toimivuutta käytännössä.

Työssäni analysoin muutamaa yleisempää jo käytössä olevaa ratkaisua. Pohdin myös yrityksen näkökulmasta sen tietoturvapolitiikan perusteella virtualisoidun työasemaratkaisun turvallisuutta. Käytän opinnäytetyössäni tekniikoita, joilla edellä mainittuun kysymykseen on vastattu muiden teknologioiden osalta. Nämä teknologiat eivät liity suoraan virtualisoituihin työasemiin. Olen pyrkinyt käyttämään opinnäytetyössäni myös luovaa ajattelua teknisen suorittamisen lisäksi. Varsinkin työssäni teknisissä tukitehtävissä olen huomannut töiden olevan usein teknistä suorittamista luovuuden sijaan. Virtualisoidut työasemat ja palvelimet ovat jo yritysten tietojärjestelmien arkipäivää. Virtualisoinnin hyödyt esimerkiksi testiympäristöjen käyttöön kustannusten osalta ovat huomattavat. Tämä opinnäytetyö pyrkii pohtimaan myös uusia käyttöratkaisuja virtualisoinnin osalta.

Tarvitseeko työntekijä välttämättä kannettavan tietokoneen vai voidaanko se korvata esimerkiksi yritysvierailuissa ja neuvotteluissa virtualisoidulla työasemalla? Ongelmana on, että usein yritysten ja organisaatioiden tietoturvapolitiikkaan liittyy sääntö, jossa yrityksen ulkopuolinen henkilö ei saa liittää konettaan yrityksen tietoverkkoon. Mikäli vierailun kohteella ei ole tarjota avointa verkkoa vierailijalle, ei vieras pääse käyttämään esimerkiksi internetyhteyksiä, VPN-yhteyksistä puhumattakaan.

Kirjoittaessani tätä opinnäytetyötä julkaistiin muropaketti.com–portaalissa uutinen suomalaisesta Finhill Oy nimisestä yrityksestä, joka tuo käyttöjärjestelmän muistitikuille. (Kurri 2008.) Kävin Finhill Oy:n edustajan kanssa keskustelua sähköpostin välityksellä opinnäytetyöhöni liittyvistä aiheista ja ongelmista. Finhill Oy ei ole ratkaissut tietoturvaan liittyviä ongelmakohtia samalla tavalla kuin olen tutkimusongelmani ratkaissut

Opinnäytetyön aihe liittyy vahvasti tietoturvaan, mutta lähinnä käytännön kautta havainnoituihin puutteisiin liittyen virtualisoitua, mobiilia käyttöjärjestelmää. Opinnäytetyössä esitellään keskeiset teknologiat ongelman ympärillä, sekä pohditaan tietoturvan kannalta vaihtoehtoista teknologiaa erilaisten puutteiden korvaavana vaihtoehtona.

Olen tehnyt opinnäytetyön toimintaansa aloittavalle yritykselle. Opinnäytetyön hyödynnettävyyttä ei ole sisällytetty tutkimukseen. Yritys on anonut sille hyödyllisyysmallioikeuden. Sen saamiseksi hyödynnettävyyttä ei saa esitellä julkisesti.

Opinnäytetyö on jaettu kuuteen eri päälukuun. Johdannossa esitetään opinnäytetyön tutkimusongelma sekä tutkimusmenetelmä. Toisessa luvussa esitellään tutkimusongelman teoreettinen tausta. Kolmannessa esitellään digitaalinen oikeuksien hallinta, joka on jo askel kohti tutkimusongelman ratkaisua. Neljäs pohjustaa ja vertaa markkinoilla olevaa virtualisointiratkaisua opinnäytetyön ongelmaan. Viides luku sisältää tutkimuksen tulokset. Tuloksissa perustellaan esitetty ratkaisu. Kuudes sisältää tutkimusongelman ja aiheen johtopäätökset, sekä pohditaan niiden merkitystä. Seitsemännessä luvussa pohditaan yhteenvetona tutkimusongelman syvempää merkitystä ja esitetään mahdollisia jatkotutkimusaiheita.

1.1 Tutkimusongelma

Tässä opinnäytetyössä tutkitaan Player–nimistä virtualisointisovellusta ja sen erästä ominaisuutta, joka on luotu helpottamaan sovelluksen käyttöä. Sovelluksen ominaisuuteen liittyvän tietoturvaongelman tuo esiin työntekijän ja mobiilin virtualisoidun koneen siirtyminen paikasta A paikkaan B, koska siirtyminen paikasta toiseen ei vaadi virtualisoidun työaseman sulkemista kokonaan. Ongelma syntyy virtuaalisovelluksen ominaisuudesta, jossa virtuaalisovelluksen sulkeminen ei aja käyttöjärjestelmää alas, vaan se menee niin kutsuttuun nukkumistilaan.

Yritysten työasemat ovat usein tietoturvapolitiikan mukaisesti suojattu käyttäjän autentikoinnilla ja mahdollisesti muilla tekniikoilla, esimerkiksi tietoliikenteen osalta. Virtuaalisovelluksen sulkeminen nukkumistilaan ei sitä uudelleen avattaessa vaadi autentikointia käyttöjärjestelmän eikä salattujen VPN yhteyksien osalta kuten normaalin käynnistyksen yhteydessä.

Edellä mainittu ominaisuus itsessään ei ole ongelma. Kyseinen ominaisuus on luotu helpottamaan ja nopeuttamaan käyttöjärjestelmän käytettävyyttä. Ongelma tulee esiin nimenomaan yritysmaailmassa tai henkilöiden kohdalla, jotka haluavat suojata virtualisoitua tietokonettaan. Kun virtualisoitu käyttöjärjestelmä VMware Playeriä käyttäen on nukkumatilassa, sen kopioiminen on mahdollista. Kopioitu, nukkumatilassa oleva käyttöjärjestelmä avautuu täysin samalla tavalla kuin alkuperäinen virtualisoitu käyttöjärjestelmä, ilman autentikointeja. On-

gelma on siis tietoturvan näkökulmasta perustavanlaatuinen. Yleisesti työtekijät haluavat käyttöjärjestelmän ja muut yrityksen työkalut käyttöön missä tahansa, milloin tahansa ja median voi kantaa helposti mukana. Tietoturvaa pohtiessa on kyseisen soveluksen ongelma niin suuri, että ilman sen selvittämistä tuotetta ei voi käyttää yritysratkaisuissa tai missään vastaavissa ympäristöissä, joissa on pääsy arkaluontoiseen tietoon tai resurssiin.

On olemassa medioita, joilla käyttäjien tunnistaminen tapahtuu mekaanisesti, esimerkiksi sormenjälkitunnistuksella varustettu ulkoinen kovalevy, mutta sitä käytettäessä tulee yritykselle taas uusi tuote hankittavaksi. Yksi lähtökohdista on, että käyttöjärjestelmä voidaan asentaa mille tahansa kannettavalle medialle: esimerkiksi mp3-soittimelle, puhelimeen, muistitikkulle tai muistikorttiin, joita yrityksissä yleensä on jo valmiiksi.

1.2 Tutkimusmenetelmä

Tutkimusmenetelmä on suunnittelutieteellinen tai konstruktiivinen tutkimus. Siitä käytetään myös nimitystä soveltava tutkimus. (Järvinen & Järvinen 2004, 103.) Järvisen ja Järvisen mukaan suunnittelutieteen tarkoitus on joko luoda tietämystä suunnittelua ja toteutusta eli konstruktio-ongelmien ratkaisua varten tai parantaa nykyisten systeemien suorituskykyä (Järvinen & Järvinen 2004, 103.)

Olen opinnäytetyössäni ottanut mallia virtuaalikoneen suojaamiseksi DRM-teknologioista, joita käytetään muissa kohteissa, kuten mp3-tiedostojen ja PDF-dokumenttien suojaamisessa. Olen esittänyt tuloksena ratkaisun, jossa DRM-tekniikkaa hyödynnetään sovelletuin osin virtualisoidun, mobiilin käyttöjärjestelmän suojaamiseksi.

Tutkimuksessani olen kiinnostunut ongelmasta sen toiminnan merkityksen ymmärtämiseksi. Ongelmani on tullut esiin työympäristössä normaalin toiminnan yhteydessä. Tutkimusmenetelmäni on teoriassa tapaustutkimusta. Tapaustutkimuksessa on tavoitteena juuri toiminnan merkityksen ymmärtäminen tai tulkinta. (Hirsjarvi ym. 1997, 130-131). Tapaustutkimus on yksityiskohtaista, intensiivistä tietoa yksittäisestä tapauksesta tai pienestä joukosta toisiinsa suhteessa olevia tapauksia. Tyypillisesti valitaan yksittäinen tapaus, tilanne tai joukko tapauksia, jossa yksittäistapausta tutkitaan yhteydessä ympäristöönsä. Ympäristöllä tarkoitetaan luonnollista tilannetta, jossa tutkittava tapaus on. Tapaustutkimuksessa aineistoa kerätään useita metodeja käyttämällä, kuten havainnointi, haastattelut ja dokumenttien tutkiminen. Tavoite tapaustutkimuksille on tyypillisimmin ilmiöiden kuvailu. (Hirsjärvi ym. 1997, 130-131).

Tutkimusaineistona on käytetty keskusteluja, dokumentteja sekä kirjallisuutta. Keskusteluissa on tullut esiin asiantuntijoiden suosittelemia dokumentteja. Olen näitä dokumentteja tutkiessani saanut enemmän käsitystä yleisesti kokonaiskuvista liittyen suojauksiin liittyvissä asiois-

sa. Olen kerännyt tietoa myös vastaavasta tuotteesta, joka on vertailukohteena opinnäytetyössä käytettyyn sovelluksiin ja sen ratkaisuille. Tieto vertailukohteena olevasta tuotteesta on saatu sähköpostikeskustelujen ja niissä esitettyjen kysymysten kautta.

2 Tutkimuksen teoria

Tässä luvussa esitetään tutkimuksen teorian keskeiset asiat, jotka liittyvät pääosin virtualisointiin, käyttäjän autentikointiin ja tietojen suojaamiseen.

2.1 Virtualisointi

Virtualisointi tietotekniikassa tarkoittaa resurssin tai palvelun erottumista alemmasta fyysisestä resurssista (Kuvio 1). Tietokoneissa resurssien kerrokset tarkoittavat siis laitteen rakennetta fyysisestä laitteesta sovellukseen asti. Esimerkiksi virtuaalimuistin avulla käyttöjärjestelmä saa enemmän keskusmuistia kuin mitä tietokoneeseen on fyysisesti asennettu. Virtuaalimuisti todellisuudessa on massamuistilaitteella ja virtuaaliosoitteet mahdollistavat sen käytön. (Virtualization Overview 2006, 3.)

Virtuaaliosoitteet eivät kuitenkaan tarkoita, että ne olisivat virtualisointijärjestelmä. Samalla tekniikalla pystytään käyttämään virtualisointiratkaisuja muihin IT-infrastruktuurin kerroksiin, kuten verkkoihin, tallennusjärjestelmiin, kannettaviin tietokoneisiin, palvelimiin, käyttöjärjestelmiin ja sovelluksiin. Virtualisoitu infrastruktuuri tuottaa abstraktin kerroksen eri osa-alueiden välille. Virtualisoitu infrastruktuuri ei myöskään aiheuta häiriöitä tai muutoksia loppukäyttäjälle esimerkiksi laitevioista verrattuna tavalliseen palvelinratkaisuun. (Virtualization Overview 2006, 3).

Virtualisoinnin hyöty tulee esiin järjestelmien hallinnan osalta. Tavanomaisessa palvelinympäristössä hallinnoidaan esimerkiksi viittäkymmentä palvelinkonetta. Virtualisoidussa palvelinympäristössä hallinnoidaan esimerkiksi yhtä fyysistä laitetta, jonka sisällä on virtualisoituna useampi ”palvelin” (Kuvio 1). Järjestelmänvalvojien on helpompi hallinnoida resursseja kokonaisuutena yhden laiteratkaisun osalta verrattuna viiteenkymmeneen laitteeseen. Virtualisointi myös parantaa infrastruktuurin dynaamisuutta, koska palvelimet eivät ole riippuvaisia fyysisestä laitealustasta. Virtualisoitu kone ei ”näe” suoraan fyysistä laitetta. (Virtualization Overview 2006, 3).

Kuvio 1: Palvelinvirtualisointi (Virtualization Basics 2008.)

2.2 Virtualisointi x86-alustalla Windows-ympäristössä

Virtualisointi on ollut osa IT-järjestelmiä jo vuosikymmeniä esimerkiksi finanssisektorilla ja pankeissa. Kriittiset järjestelmät halutaan pitää toiminnassa laiteviasta huolimatta. Yleisin käyttötapa aikaisemmin oli kahdentaa laitteet, kuten esimerkiksi kovalevyjen RAID-ratkaisuissa. Vasta 90-luvun lopussa VMware-niminen yritys tutki x86-alustan virtualisoimisen hyötyjä. (Virtualization Overview 2006, 4-5.)

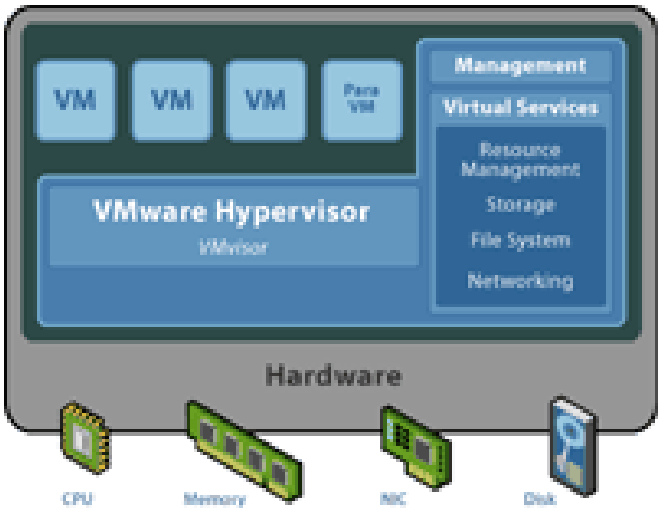
X86-alusta on yleinen nimi Intelin kehittämälle suoritinarkkitehtuurille. Kaikki ”personal computeriksi” eli PC:ksi nimettyjen henkilökohtaisten tietokonearkkitehtuurien mukaiset tietokoneet käyttävät x86-arkkitehtuurin mukaisia suorittimia.

Yksi päähyöty virtualisoinnissa on ajaa useita käyttöjärjestelmiä samanaikaisesti yhdellä laitealustalla. Konetehojen lisääntyessä laiteresursseja jää vapaaksi. Virtualisoinnilla pyritään parantamaan resurssien tehokkaampaa käyttöä. Tätä virtualisoimista kutsutaan vapaasti käännettynä nimellä käyttöjärjestelmien ”partitiointi”. (Virtualization Overview 2006, 4.)

Fyysisten laitteiden virtualisoinnin eli klusteroinnin yleinen käyttö 70-luvulla oli pääosin IBM:n keskuskoneratkaisuissa. UNIX oli ensimmäinen järjestelmä joka pystyi virtualisoimaan käyttöjärjestelmiä ja sovelluksia eri laitealustoilla. (Virtualization Overview 2006, 4.)

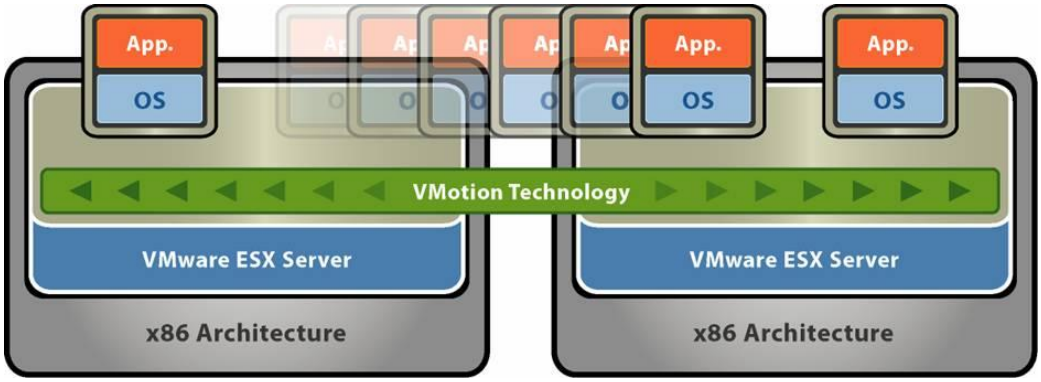
Unixin ja x86-järjestelmien partitiointi perustuu kahteen eri arkkitehtuuriin; hypervisor-arkkitehtuuriin ja niin sanottuun isäntä-arkkitehtuuriin. Isäntä-arkkitehtuurin idea perustuu ”host”–käsitteeseen, jossa esimerkiksi käytetään monta käyttöjärjestelmää fyysisen resurssin päällä. (Virtualization Overview 2006, 4.)

Fyysinen resurssi on käyttöjärjestelmien isäntä eli ”host”. Virtualisoinnissa isäntä-arkkitehtuurissa normaalin käyttöjärjestelmän päälle luodaan alusta, jonka päällä toimii virtualisointi-kerroksen avulla partitioitu ratkaisu. Verrattuna hypervisor-ratkaisuun, isäntä-arkkitehtuurissa on isäntä-käyttöjärjestelmä, jonka päällä on virtualisointikerros. Hypervisor-ratkaisuissa virtualisointikerros on suoraan fyysisen resurssin päällä (Kuvio 2). Isäntä-arkkitehtuurin virtualisointikerros on siis altis isäntä-käyttöjärjestelmän vikaantumiselle. (Virtualization Overview 2006, 4-5.)



Kuvio 2: Hypervisor virtualisointi 1 (Transparent Paravirtualization 2008.)

Hypervisor-ratkaisu on ensimmäinen sovelluskerros puhtaan x86-alustan päällä. Tätä kutsutaan myös nimellä ”bare metal”-asennus. Koska hypervisor-virtualisointialustalla on suora yhteys fyysiseen laiteresurssiin, on hypervisor ratkaisuna isäntä-ratkaisuun verrattuna huomattavasti varmatoimisempi, skaalautuvampi ja tehokkaampi (Kuvio 3). (Virtualization Overview 2006, 4-5.)

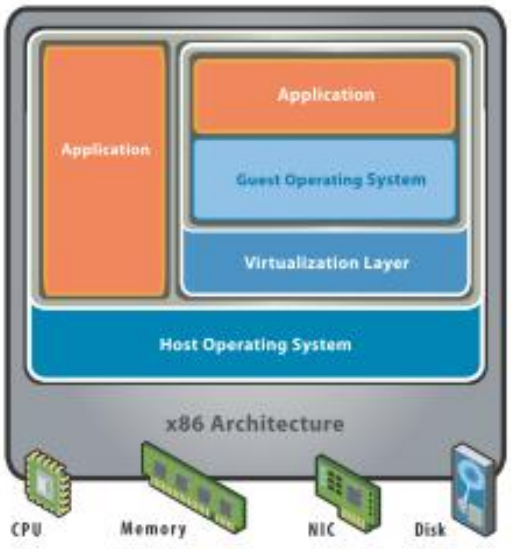


Kuvio 3: Hypervisor virtualisointiklusteri (VMware VMotion 2008.)

Hypervisor-ratkaisun hyötyjä ovat myös virtualisoitujen käyttöjärjestelmien eristyneisyys toisistaan ja riippumattomuus fyysisestä laitealustasta. Virtualisoitu käyttöjärjestelmä voidaan siirtää eri x86-laitealustalta toiseen riippumatta valmistajasta ja mallista, mikäli molemmissa on asennettuna virtualisointikerros. (Virtualization Overview 2006, 4-5)

2.3 Para–virtualisointi

Para-virtualisoinnin sana ”para” tulee englannin kielestä ”parallel” ja perustuu kreikan kieleen. ”Parallel” tarkoittaa vapaasti käännettynä ”rinnalla”, ”kanssa” tai ”mukana”. Vapaasti tulkittu sanamuoto ”rinnakkais-virtualisointi” kuvaa para-virtualisoinnin teoriaa. Virtualisoitu kerros toimii isäntä-käyttöjärjestelmän päällä (Kuvio 4). Hypervisor-kerros keskustelee käyttöjärjestelmän kanssa, eikä suoraan fyysisen laitekerroksen päällä kuten tavallinen hypervisor - virtualisointiratkaisu. (Understanding Full Virtualization, Paravirtualization, and Hardware Assist 2007, 5).



Kuvio 4: Para-virtualisointi (Paravirtualization 2007.)

2.4 VMware Player

Tässä opinnäytetyössä käytetään yhtä suurinta x86-alustalle keskittynyttä para-virtualisointi ratkaisua, VMWaren Player -nimistä ilmaisohjelmaa, jolla pystytään ajamaan virtualisoitua käyttöjärjestelmää Windows XP -käyttöjärjestelmän sisällä. VMware tarjoaa myös ilmaiseksi työkalu- ja ajuripaketin VMware Player -asennuspaketin mukana. Näillä ajureilla pystytään käyttämään isäntä-käyttöjärjestelmän fyysisiä resursseja, kuten verkkokortteja, usb-portteja näytönohjainta riippumatta sen valmistajasta tai mallista. Virtualisoitu käyttöjärjestelmä toimii Windows alustalla kuten mikä tahansa muu sovellus. VMWare tuottaa myös maksullisia para-virtualisointi sovelluksia, jotka ovat ominaisuuksiltaan hieman monipuolisempia kuin Player -sovellus. (Getting Started Guide: VMware Player 2.0 2007, 7)

VMware Player on kehitetty sovelluksena tarjoamaan sen käyttäjälle välineen testata eri käyttöjärjestelmien ominaisuuksia. Sillä voi helposti asentaa virtuaalisen käyttöjärjestelmän ja kokeilla eri sovellusten toimivuutta uuden käyttöjärjestelmän päällä. Esimerkiksi organisaati-

oissa voidaan uuden käyttöjärjestelmän sukupolvenvaihdoksen yhteydessä kokeilla etukäteen eri järjestelmien toimivuutta uudessa käyttöjärjestelmässä.

2.5 Mobiililaitteet

90-luvulle asti kaikki yritysten ulkoinen kommunikaatio käsitti pääosin ainoastaan posti- ja puhelinjärjestelmät. Puhelinjärjestelmiä olivat äänipuhelimet sekä faksit. Nykypäivänä järjestelmät ovat vaihtuneet kannettaviin tietokoneisiin, sähköpostiin, Internet-sovelluksiin ja mobiililaitteisiin jotka yhdistyvät langattomasti tietoverkkoihin. (Laudon & Laudon 2006, 262).

Vuonna 2004 on arvioitu, että Yhdysvalloissa lähetettiin päivittäin noin miljardi tekstiviestiä, neljä miljardia sähköpostia, sekä miljoonia taulukoita ja dokumentteja. Maailmanlaajuisesti vuonna 2004 investoitiin telekommunikaatiolaitteisiin arvioidusti 2.2 triljoonaa dollaria ja määrän arvioitiin kasvavan kolmeen triljoonaan euroon vuonna 2007. (Laudon & Laudon 2006, 262).

Mobiiliratkaisuiden tarkoitus yritysmaailmassa on mahdollistaa työntekijöiden, asiakkaiden ja toimittajien kommunikaatio milloin hyvänsä, mikäli se katsotaan tarpeelliseksi, suoriutuakseen työstään. Telekommunikaatio ja mobiililaitteet mahdollistavat yhteyden tarpeen vaatiessa lokaatiosta riippumatta. Käytännössä se ei välttämättä kuitenkaan toimi niin, johtuen esimerkiksi langattomien verkkojen katveista tai teleoperaattorin yhteyksien katveista. (Laudon & Laudon 2006, 262).

2.6 VPN

VPN eli Virtual Private Network on teknologia, jolla yritys voi yhdistää kaksi tai useampia yrityksen tietoverkkoja julkisen verkon yli muodostaen näennäisesti yksityisen verkon. VPN-määritelmä koskee myös yksittäisten etätyöaseman tai mobiililaitteen liittämistä yrityksen verkkoon. Internet protokollaan perustuva VPN-ratkaisu tarjoaa suojatun yhteyden julkisessa internet-verkossa näiden kahden tai useamman pisteen välille.

Internet Protokollaan perustuva VPN-ratkaisu mahdollistaa huomattavia säästöjä verrattuna yksityiseen verkkoratkaisuun, eikä yhteys ole rajattu nopeudeltaan yrityksen omaan verkkokapasiteettiin. Se helpottaa myös eri maanosissa olevien toimipisteiden yhdistämistä toisiinsa, verrattuna fyysiseen yksityiseen yritysverkkoon eri maanosien välillä. (Laudon & Laudon 2006, 291-292).

2.7 Tietojen Suojaus

Käyttäjien hallinta yritysten tietojärjestelmissä on käytäntöjä ja prosesseja, joita organisaatio käyttää estämään tietojärjestelmien sopimatonta ja luvatonta käyttöä yrityksen sisällä ja sen ulkopuolella. Jotta käyttäjä pääsee käsiksi haluamiinsa tietoihin tai resursseihin, tulee hänet tunnistaa ja autentikoida. Autentikointi eli käyttäjien varmennus tarkoittaa kykyä tunnistaa henkilö siksi henkilöksi, joka hän väittää olevansa. (Laudon & Laudon 2006, 362).

Esimerkiksi pankkiautomaateilla tunnusluvulla varmennetaan kortin omistaja ja kortin luvallinen käyttö. Sovellukset käyttäjien hallintaan on suunniteltu antamaan tietylle henkilölle pääsy tietoihin ja resursseihin perustuen ennalta hyväksyttyyn tunnistusprosessiin, esimerkiksi juuri pankkikortin PIN-koodi.

Käyttäjien hallinta –käsitteenä tietojärjestelmissä on pääasiassa käyttäjätilit ja niiden avaamiseen tarkoitetut salasanat. Henkilö käyttää salasanaa kirjautuessaan järjestelmiin ja mahdollisesti vielä sen jälkeen tiettyyn tietoon. Käyttäjät valitettavasti unohtavat salasanojaan, luovuttavat salasanansa kollegoilleen tai valitsevat liian helppoja salasanoja itselleen, jolloin yrityksen tietoturvan perustaso laskee.

Käyttäjätilien varmentamiseksi voidaan myös ottaa käyttöön sirukortteja tai muita vastaavia älykortteja käyttäjien tunnistamiseen. Biometriset tunnisteet ovat seuraavan sukupolven tunnistusmetodeja, jotka parantavat autentikointiprosessia ja yrityksen tietoturvaa huomattavasti verrattuna salasanoihin tai älykortteihin. (Laudon & Laudon 2006, 363).

Biometrisiä tunnistusmetodeja ovat sormenjälki tai verkkokalvotunnisteet. Biometristen tunnistemetodit ja laitteet ovat kalliita verrattuna käyttäjätileihin ja älykortteihin, johtuen kehittyneemmästä teknologiasta. Tavallisissa organisaatioissa niitä ei yleensä käytetä johtuen hankintojen kalleudesta. (Laudon & Laudon 2006, 363).

Useimmat organisaatiot ja yritykset luottavat tiedon kryptausmenetelmiin suojatakseen luotettavia tietoja. Kryptaus on salauskoodi mikä liitetään haluttuun tietoon tai resurssiin. Tällä salauksella pyritään estämään tiedon tai resurssin luvaton käyttö. Esimerkiksi sähköposti voidaan suojata salausavaimella ja vastaanottaja voi oikealla avainkoodilla tai salasanalla avata kyseisen salatun viestin. (Laudon & Laudon 2006, 365).

2.8 Virtuaalikoneen Suojaus

Virtualisoitu käyttöjärjestelmä muistitikulla sisältää käytännössä käyttäjän autentikoinnin ja VPN–yhteyden yrityksen sisäverkkoon miltä tahansa tietokoneelta. Käyttöjärjestelmä on asennettu ja konfiguroitu kuten yrityksen muut fyysiset koneet.

Käytettävä tietokone voi olla esimerkiksi kahvilan tai kirjaston yleiskone, jossa VMPlayer-sovelluksella avataan virtualisoitu käyttöjärjestelmä ja siitä suojattu yhteys yrityksen verkkoon VPN-sovelluksella.

Ongelmaksi tässä yhtälössä muodostuu VMPlayerin ominaisuus, jossa sovelluksen sulkeminen ei sulje virtualisoitua käyttöjärjestelmää vaan laittaa sen ns. ”hibernate”-tilaan. Hibernate tilaa on kutsuttu myös ”nukkuvaksi”-tilaksi. Käytännössä käyttäjä kirjautuu koneelle, jolloin käyttäjän autentikointi tapahtuu sekä tietokoneelle, että yrityksen verkkoon. VPN–yhteyden autentikoinnin jälkeen on käyttäjällä mahdollisuus käyttää konetta kuten mitä tahansa muuta työkonetta, joka olisi normaalisti yrityksen sisäverkossa. Kaikki henkilölle määritelty tieto ja resurssit ovat käyttäjän saatavilla.

Suljettaessa virtualisointiohjelmaa, Player–sovellus ei sulje käyttöjärjestelmää vaan laittaa sen hibernate–tilaan. Mikäli halutaan sulkea myös virtualisoitu käyttöjärjestelmä, pitää se erikseen niin tehdä. Virtuaalikone avattuna uudelleen missä tahansa lokaatiossa hibernate -tilasta avaa käyttöjärjestelmän samaan tilaan, kuin missä se on edellisen kerran suljettu. Autentikointia ei tehdä uudelleen, VPN–yhteys muodostuu automaattisesti uudelleen, sulkemishetkellä avoimet sovellukset ovat samassa tilassa kuin sulkiessa. Jopa hiiren osoitin on samassa kohdassa kuin sovelluksen sulkemishetkellä. Mitään autentikointia ei tehdä uudelleen, ellei itse käyttöjärjestelmää ole suljettu erikseen.

Virtualisoitu kone muistitikulla on käytännössä muutama tiedosto, joiden kopioiminen on helppoa. Muistitikulle tallentuu virtuaalikoneen hallintatiedostoja, sekä yksi image–tiedosto jossa käyttöjärjestelmä itsessään sijaitsee. Tuo image–tiedosto simuloi tietokoneen kovalevyä. Hibernate-tilassa kopioidut tiedostot avautuvat ilman autentikointia edelleen myös kopioidulta medialta ja tämä on tietoturvan kannalta suuri riski. Muistitikun suojaaminen kryptaamalla ei välttämättä tarjoa riittävää suojaa.

2.9 Digitaalinen Käyttöoikeuksien Hallinta

DRM on suojausteknologia, jonka päätarkoituksena on hallinnoita tai rajoittaa tiedon käyttöä. DRM –suojaukset ovat suuresti käytössä elektronisten kirjojen, musiikkikappaleiden ja musiikkitallenteiden suojauksissa.

Käytännössä DRM-suojaus poistaa käyttäjältä oikeuden kontrolloida suojattua tiedostoa. Käytetty DRM-sovellus hallinnoi oikeuksia kyseiseen tiedostoon. Käyttökohteet ovat ainakin teoriassa loputtomia. Käytännössä valmiita DRM -sovelluksia ei ole kaikille mahdollisille tiedostopäätteille tai tiedostotyypeille.

Yritys voi esimerkiksi estää suojatun sähköpostin välittämisen eteenpäin hyödyntäen DRM-teknologiaa. Elektroninen kirja voidaan suojata, jolloin sen kopioiminen ja tulostaminen on estetty tekijänoikeuden omistajan toimesta.

Elokuva DVD:n kopioiminen voidaan estää DRM–suojauksella kokonaan tai kopioiden määrä rajoitetaan esimerkiksi kahteen kopioon. CD-levyllä oleva musiikkiäänite voi sisältää ylimääräistä tietoa, jolloin kopioimiseen tarkoitettu sovellus ei pysty kopioimaan äänitettä.

2.10 Kuluttajien Kritisoima

Vaikka kuluttajat ovat mediassa ja keskustelufoorumeilla kritisoineet DRM-ratkaisuja liian rajoittaviksi ratkaisuiksi erityisesti elokuva DVD–levyjen ja musiikki–cd:n osalta, DRM-sovellukset pyrkivät ratkaisemaan realistisen ongelman. Electronic Frontier Finland ry, joka on perustettu puolustamaan kansalaisten sähköisiä oikeuksia internetissä, kuvailee DRM – lyhennettä yhteisnimityksenä kaupallisesti motivoidulle tekniselle rajoitteelle digitaaliseen tiedonsiirtoon. He ovat esittäneet nimen Digital Rights Management muuttamista Digital Restrictions Managementiksi. (EFFI 2008).

Internetin välityksellä toimiva laiton jakelu vertaisverkoissa teki perinteisen tekijänoikeuslain riittämättömäksi tavaksi suojata tekijänoikeuksilla suojattua materiaalia. Joka kerta kun henkilö lataa internetin välityksellä laittomasti tekijänoikeuden alaisen kappaleen mp3-musiikkitiedostona koneelleen, tekijänoikeuden omistava yritys ja samalla muusikot itse häviävät rahaa, jonka he perinteisesti kaupasta ostetusta musiikkiteoksesta saavat.

Motion Picture Association of America, eli Yhdysvaltojen elokuvateollisuuden pääorganisaatio on laskenut tuottojen laskeneen noin viisi miljardia dollaria vuodessa johtuen piratismista ja laittomasti ladatuista elokuvista. (MPAA 2005).

Internet tietoverkkona tekee teoriassa mahdottomaksi saattaa jokainen laittomasti lataava henkilö vastuuseen rikkoessaan lakia. Yritykset itse ovat muuttaneet toimintatapojaan materiaalin jakelussa tekemällä kuluttajien suorittaman digitaalisen kopioimisen mahdottomaksi hyödyntäen erityisesti DRM -teknologioiden tuomia ratkaisuja.

Kuluttajat pitävät ongelmakohtana laillista oikeuttaan tehdä esimerkiksi elokuva DVD:stä kopiota itselleen. DRM–sovellukset eivät erota kopioidun materiaalin käyttökohdetta. Sovellus ei tiedä mihin käyttöön kopio tulee.

2.11 DRM:n Runko

Ideaalinen DRM–sovellus on käyttäjälle joustava, täysin läpinäkyvä ja rakenteeltaan melko monimutkainen ymmärtää muiden tietokoneen sovelluksien toimesta. Ensimmäisen sukupolven DRM–sovellukset pyrkivät ainoastaan kontrolloimaan tiedon kopioimista. (Layton 2006).

Toisen sukupolven sovellukset ovat tällä hetkellä vielä kehitysvaiheessa tai niin sanotusti lasten kengissä kaikilta osa-alueilta, joita pyritään hallitsemaan. Sovellukset halutaan kontrolloivan katselua, kopioimista, tulostamista, muokkaamista ja itse asiassa kaikkia digitaalisen sisällön operaatioita. (Layton 2006).

DRM–sovellukset toimivat kolmella kerroksella: muodostamalla tekijänoikeuden kyseiseen tietoon, hallinnoimalla tekijänoikeuden alaisen tiedon jakelua ja kontrolloimaan mitä operaatioita tiedolla voidaan tehdä. Esimerkiksi DRM- tekniikalla suojatun, luottamukselliseksi luokitellun dokumentin tulostamista voidaan rajoittaa, tai se voidaan estää kokonaan. DRM-sovelluksen tulee määritellä kolme kokonaisuutta: käyttäjä, sisältö ja käyttöoikeus suojattuun tietoon. Näiden kolmen instanssin suhde ja oikeudet toisiinsa tulee määritellä sovelluksen toimesta. Käyttäjäinstanssille voidaan määritellä mitä sisältöä se saa tiedosta näkyville ja miten sitä tietoa voi käsitellä. (Layton 2006).

Esimerkiksi käyttäjä nimeltä Eero Arte ostaa verkkokaupasta mp3-musiikkitiedoston. Rekisteröityessään verkkokaupan asiakkaaksi hän saa esimerkiksi ladata viisi musiikkitiedostoa kuukaudessa ilmaiseksi. Verkkokaupan käyttäjien hallinta luo asiakkaalle asiakasnumeron rekisteröitymisen yhteydessä. Jokaisella verkkokaupan musiikkitiedostolla on uniikki tuotenumero, joka erottelee sen muista tiedostoista.

DRM–sovelluksella suojatussa mp3-tiedostossa voidaan määritellä, voiko asiakas kopioida tiedoston, voiko tiedostoa avata millään muulla kuin verkkokaupan omalla toisto-sovelluksella, voiko tiedostoa lähettää sähköpostilla eteenpäin tai voiko tiedostoa siirtää esimerkiksi kannettavaan mp3-soittimeen. Verkkokauppa itse voi myös tarjota asiakkaalle lisämaksusta sa-

man tiedoston eri oikeuksilla. Lisämaksusta asiakas voi ladata tiedoston myös kannettavaan soittimeen. DRM – sovelluksella määritellään itse musiikkitiedostoon käyttäjä, tiedosto itsessään ja käyttäjän oikeudet tuohon tiedostoon.

2.12 DRM ja iPod

Applen valmistama iPod on kiintolevyllinen tai flash –muistillinen, kannettava musiikkisoitin. Se toistaa useita eri formaatin musiikkitiedostoja, joita hallinnoidaan iTunes nimisellä sovelluksella. iTunes sovellus on Applen ilmainen sovellus. Se sisältää myös ”verkkomusiikkikaupan” , josta voi ostaa musiikkikappaleita, sovelluksia ja elokuvia. (Apple, 2008)

iTunes ohjelma sykronoi kaiken sen hallinnoiman musiikkisisällön iPod –laitteeseen. DRM:n katsontakannalta iPod on ainoastaan ”dongle” iTunesille. iTunes on se instanssi johon kaikki oikeudelliset seikat aktivoidaan. Yksi iPod voidaan synkronoida vain yhden iTunesin kappaleiden kanssa kerrallaan. Tällä menetelmällä, Applen näkökulmasta, yksi ihminen voi omistaa monta musiikkisoitinta ja synkronoida ne kaikki henkilön oman iTunesin kautta. (Eran, 2006).

2.13 DRM Käytännössä

Teoriassa on melko yksinkertaista hallinnoida asiakkaan ostamaa mp3-tiedostoa ja sallia sen kopiointi esimerkiksi kolmesti. Sovellus ei kuitenkaan ymmärrä, että jos asiakas on ladannut sen koneelleen ja myöhemmin siirtänyt sen mp3-soittimeensa. Myöhemmin asiakas ostanut kannettavan tietokoneen ja haluaa siirtää kyseisen kappaleen vielä myös siihen. Hallintasovelluksiin on vaikea implementoida kopiointia omaan käyttöön, joka on suomessa lain puitteissa sallittua. Kopioiminen omaan käyttöön on sovelluksen näkökulmasta silti pelkästään kopioimista.

Yleisimpiä DRM-ratkaisuja ovat salausavaimet, jotka eivät vanhene koskaan. Salausavain sidotaan käyttäjän laitetunnukseen. Salauksen ohi pääsee ainoastaan silloin, jos tiedosto tai tieto avataan alkuperäisellä koneella, jonka laitetunnus on sidottu salausavaimeen. Jos käyttäjä kykenisi kopioimaan tai lähettämään edelleen pelkän salausavaimen ja tiedoston, ei suojauksesta ole hyötyä tietoturvan kannalta. Laitetunnus voi olla periaatteessa minkä tahansa tietokoneen komponentin tunnus. Esimerkiksi tietokoneen prosessorilla on oma uniikki laitetunnus. (Layton 2006).

Yleensä digitaalisen tiedon suojaamisessa on kyse kryptaamisesta. Kryptauksessa tosin on suojausmenetelmänä rajoitteensa. Kryptaus ei estä käyttäjää kopioimasta suojattua tietoa. Kryptatun tiedoston kopiointi on yhtä helppoa kuin suojaamattoman tiedoston kopiointi. Käyttäjä voi myös lähettää kryptatun tiedoston sähköpostilla tai jopa jakaa sen vertaisverkossa.

Kryptauksella suojattu tiedosto ei ole suojattu kopioimiselta, vaan kryptaus estää tiedoston avaamisen tai käytön.

Tämä on suurin eroavaisuus, joka selvittää perinteisen kryptaysmetodien ja DRM-ratkaisujen erot tiedostoja suojatessa. Tiedoston kontrollointi kryptauksessa tapahtuu sisällön saatavuuden kohdalla, ei esimerkiksi kopioimisen tai muiden operaatioiden osalta. Kryptauksella suojatun tiedoston voi kopioida lukemattomia kertoja, mutta kopiolla ei ole merkitystä, jos tietoon ei pääse käsiksi. Oikealla purkaus-avaimella tai salasanalla tieto tosin avautuu. Salasanalla suojattu tiedosto voidaan lähettää edelleen esimerkiksi sähköpostilla yhdessä salasanan kanssa. Vastaanottaja voi lähettää lukemattomia kertoja eteenpäin salatun tiedoston ja salasanan sen avaamiseen. Onko tiedosto edelleen suojattu?

Miten tieto voidaan jakaa ilman ”laitonta” kopiointia? DRM-ratkaisuissa salasana voidaan antaa käyttäjän tietokoneelle käyttäjän itsensä sijaan. Salasana tai purkuavain voidaan sitoa käyttäjän tietokoneessa oleviin laitetunnuksiin. Laitetunnus voi olla prosessorin tunnistenumero, kiintolevyn sarjanumero tai BIOS-tunnus. BIOS-tunnus vastaa tunnusta, kuten prosessorin laitetunnusta. (Coyle 2003.)

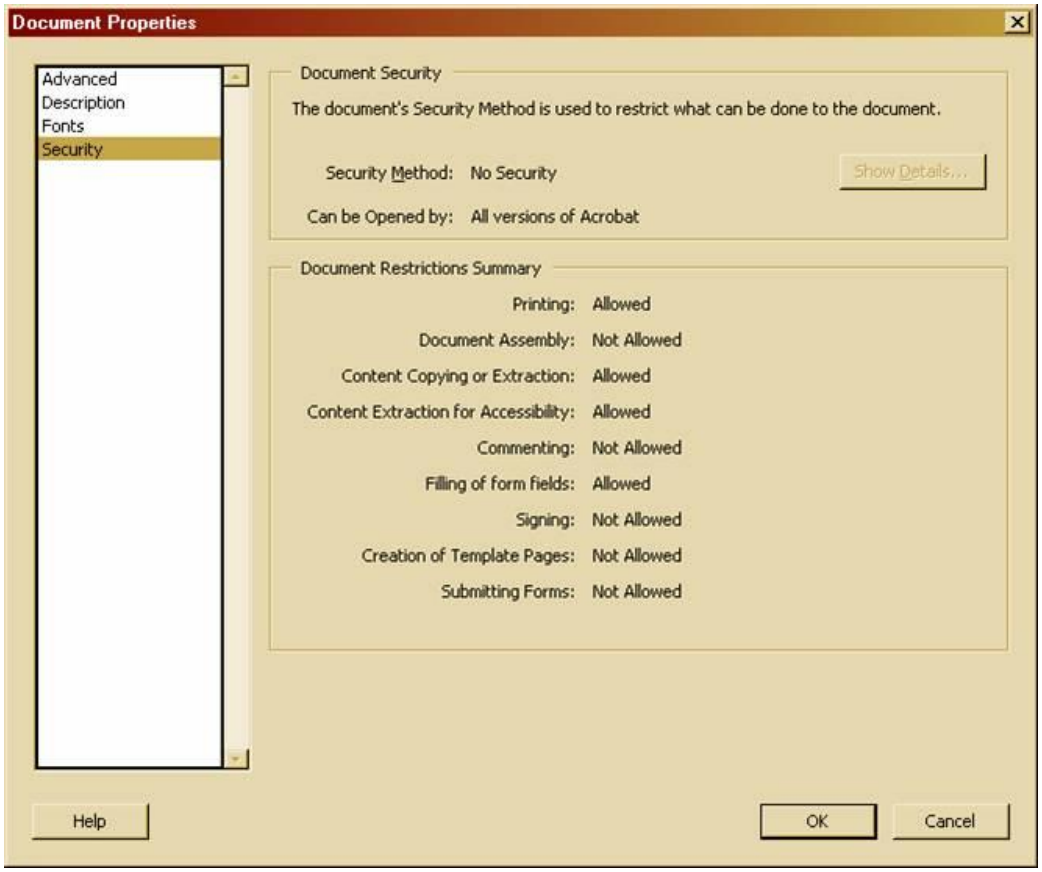
Pääkohtana on tunniste, joka on uniikki kyseiselle käyttäjälle ja jota ei pysty helposti vaihtamaan. Kun tiedostoa yritetään avata, tarkistaa se sille ennalta annetun ehdon mukaisesti laitetunnuksen koneesta. Jos tiedosto kopioidaan edelleen, kyseistä laitetunnusta ei löydy ja tiedosto ei avaudu. (Coyle 2003.)

Laitetunnukseen sidottu DRM-suojaus on yleinen ratkaisumalli DRM-suojauksissa. Ilmeinen ongelma tässä suojaustavassa on laitteiden keskimääräinen käyttöikä, joka on määritelty organisaatioiden toimesta kolmesta neljään vuoteen. Yksityisillä käyttäjillä käyttöikä on pidempi. Tällä hetkellä laitetunnukseen sidottu suojaus on kuitenkin paras ratkaisu kopioimisen estämiseen. (Coyle 2003.)

2.14 Käytön hallinta

Laitetunnukseen DRM-suojauksella sidotun tiedoston avaaminen on vasta suojauksen ensimmäinen vaihe. Tiedosto voidaan suojata myös rajoittamalla käyttäjän suorittamia operaatioita suojattuun tiedostoon. Kun tiedoston on avattu, voidaan siihen sisällyttää lisäksi esto esimerkiksi tulostaminen tai sen lähettäminen sähköpostin liitetiedostona. Tiedoston käyttöoikeus voi myös vanhentua esimerkiksi viidessä päivässä sen ensimmäisen avauskerran jälkeen. (Coyle 2003.)

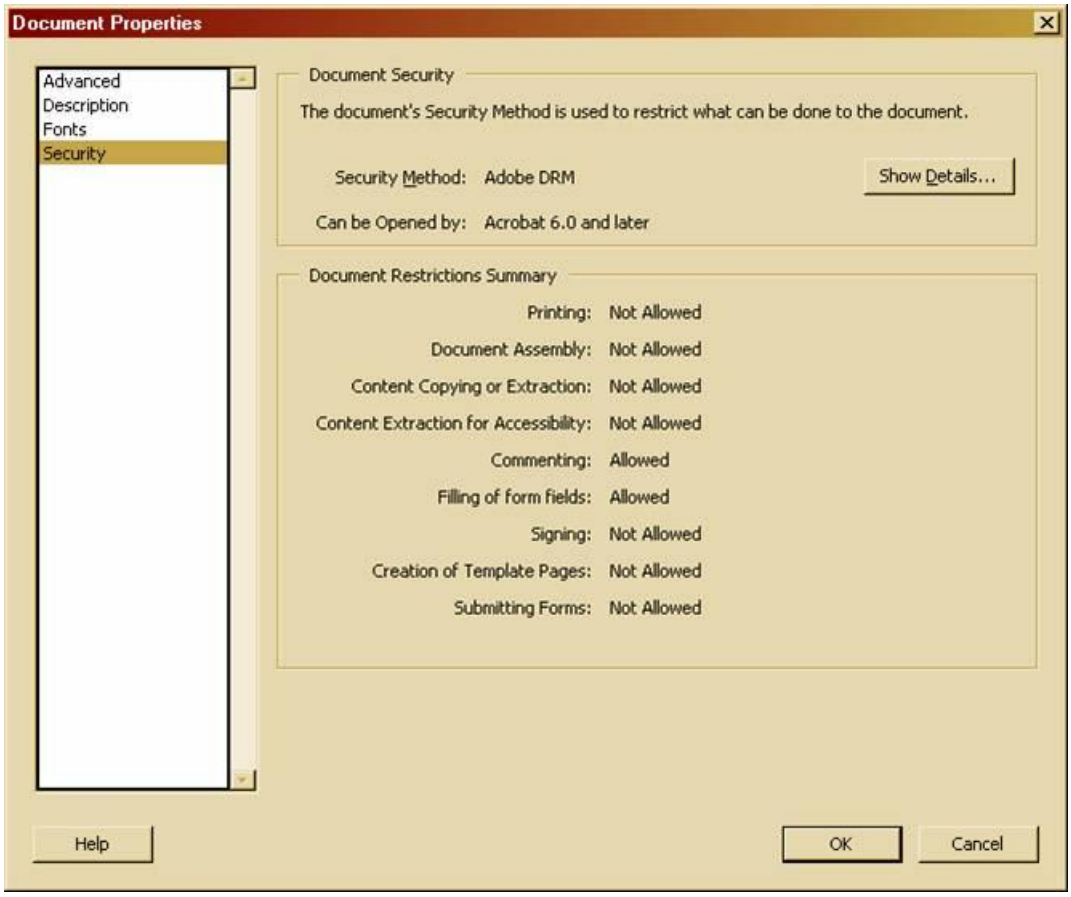
Adobe Acrobat -sovelluksessa on sisällytetty PDF-tiedostojen suojaus, joka perustuu DRM-teknologiaan. Avaamalla Acrobat -ohjelmassa valikosta tiedoston ominaisuudet, saa näkymän tiedoston ominaisuuksista liittyen tiedoston suojauksiin (Kuvio 5).



Kuvio 5: Suojaamaton Adobe Acrobat PDF-tiedosto (Coyle 2003).

Ominaisuuksista näkyy, että tiedostoa ei ole suojattu ja se voidaan avata millä tahansa Acrobatin ohjelmistoversiolla. Ikkunasta näkyy myös, että tiedoston tulostaminen on sallittu, sisällön kopioiminen on sallittu ja tekstikenttien täyttäminen on sallittu. Evätyt kohdat ovat itse asiassa sovelluksen rajoittuneisuuteen perustuvia estoja. Sovelluksella ei pysty suorittamaan kyseisiä operaatioita. (Coyle 2003.)

Suojatun tiedoston ominaisuudet tuovat seuraavat alla olevan kuvan mukaiset tiedot (Kuvio 6).



Kuvio 6: Suojattu Adobe Acrobat PDF-tiedosto (Coyle 2003).

Suojausmenetelmässä ilmenee tiedoston suojaustavaksi Adobe DRM. Tiedoston pystyy avaamaan ainoastaan Adoben 6.0 tai uudemmalla versiolla. Tiedostoon on myös määritelty operaatioihin liittyviä estoja. Tiedoston tulostaminen on estetty.

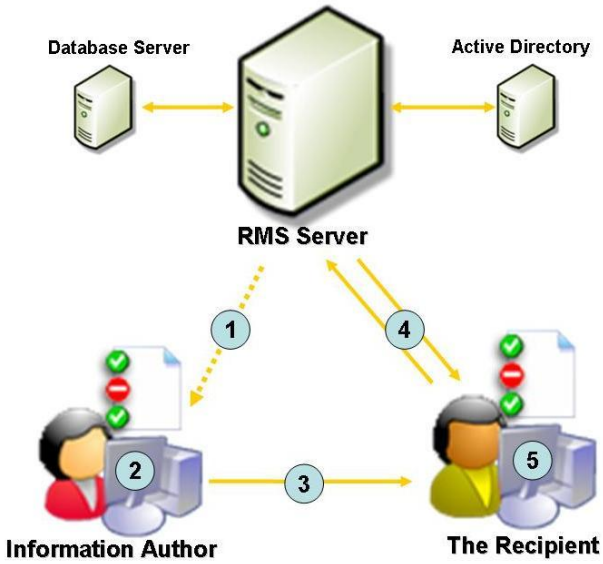
Tiedostoa avattaessa Acrobat -sovellus poistaa valikoista tulostuspainikkeet. Sisällön maalaaminen ja kopioiminen leikepöydälle on myös estetty, koko leikepöytä -ominaisuus on poistettu sovelluksesta tilapäisesti, suojatun tiedoston avaamisen yhteydessä. (Coyle 2003).

2.15 Windows Rights Management Service

Microsoft Windows Rights Management Sevice on Windows 2003 Server –käyttöjärjestelmälle luotu tiedon suojauspalvelu, joka toimii RMS-teknologialla. Rights Management Service sisältää palvelinteknologian liittää tiedostoihin sertifikaatteja ja lisenssejä, jotka määrittelevät siis oikeudet avata, käsitellä ja operoida tietoa.

Sillä voi suojata esimerkiksi Word–dokumentteja ja sähköposteja. Käyttäjä voi määritellä tiedostoon monia operaatioihin liittyviä suojauksia, kuten avaamiseen, muokkaamiseen, tulostamiseen ja välittämiseen eteenpäin liittyviä estoja. Organisaatiot voivat myös luoda omia suojausmalleja tietyn tyyppisen tiedoston käyttöön liittyvissä toimintatavoissaan. (Microsoft 2005).

Organisaatio voi luoda RMS -palvelulla keskitetysti hallinnoituja dokumentteja, kuten luottamukselliset dokumentit, joiden operaatioiden määrittelyllä on määritelty esimerkiksi ainoastaan lukuoikeuksia. Windows Rights Management Service on ilmainen lisäominaisuus Windows 2003 Server -käyttöjärjestelmän lisenssin haltijalle. (Microsoft 2005).



Kuvio 7: RMS Workflow (Microsoft 2005).

Keskitetyllä Windows RMS–palvelulla järjestelmänvalvojat voivat luoda erilaisia määrittelyjä dokumenttien osalta, sekä määritellä käyttäjäkohtaisia oikeuksia tietoihin. Määrittelyn perustana voi olla useita eri kriteereitä, kuten käyttäjätunnus, laitetunnus tai IP-osoite. (Microsoft 2005).

Itse tietoon, esimerkiksi Word–dokumenttiin lisätään lisenssitieto, jossa määrittelyt RMS-suojauksesta ja sen ominaisuuksista sijaitsevat. Tässä tapauksessa se sisältää tiedon RMS–palvelimen määrittelyt, josta itse oikeudet tietoon tarkistetaan. (Microsoft 2005).

Kun käyttäjä avaa suojatun tiedoston, RMS-palvelimelle lähtee internetverkon välityksellä tiedustelu oikeuksista. Organisaation ulkopuolella kysely tapahtuu julkisen internetverkon kautta. RMS-palvelin tarkistaa, mitä oikeuksia käyttäjällä on kyseiseen tietoon ja palauttaa tiedon määritellyistä oikeuksista. Palautetun tiedon perusteella käyttäjä voi käsitellä tietoa

määriteltyjen oikeuksien perusteella. Mikäli lisenssimäärityksissä käyttäjällä ei ole minkäänlaisia oikeuksia tietoon, RMS-palvelu ei anna oikeuksia avata tiedostoa. (Microsoft 2005).

RMS–suojatun tiedoston lisenssitiedossa voi lisäksi olla lista kriteereistä, joilla kysely oikeuksista tapahtuu. Mikäli kriteerit eivät täyty, ei kyselyä oikeuksista edes tapahdu.

3 Case Tikux – Findhill Oy

18.3.2008 julkaistiin muropaketti.com –sivustolla uutinen Tikux –nimisestä tuotteesta, jonka tuottaa turkulainen Findhill Oy. Ohjelmiston avulla voidaan asentaa Windows- tai Linux-käyttöjärjestelmä muistitikulle tai ulkoiselle kiintolevylle. Tikux -ohjelmisto perustuu virtualisointitekniikkaan, jonka ansiosta käyttöjärjestelmä toimii riippumattomana fyysisestä kokoonpanosta, tietokoneesta toiseen siirrettynä, ilman uusia ajuriasennuksia. (Kurri 2008).

Findhill Oy:n tuotteet vastaavat tarpeeseen tehdä töitä tai käyttää tietokonetta mistä tahansa ilman internetyhteyttä. Internetselaimen kautta tapahtuva etäkäyttösovellus mahdollistaa myös tarpeen, mutta se vaatii aina internetyhteyden. Tietokone johon etäyhteys otetaan, täytyy myös olla saatavilla. (Löytömäki 2008).

Tikux-ohjelmisto on rakennettu Linux–ytimen päälle ja käyttää QEMU-nimistä avoimeen lähdekoodiin perustuvaa virtualisointialustaa. Loppukäyttäjä ei käytännössä näe käyttävänsä Linuxia, koska Linuxin perusta toimii ainoastaan virtualisointialustana. Käyttäjä näkee ainoastaan virtualisointialustan päällä toimivan käyttöjärjestelmän, jonka käyttäjä on itse asentanut, esimerkiksi Windows XP –käyttöjärjestelmän. (Löytömäki 2008).

Käyttäjän asentama virtuaalikäyttöjärjestelmä toimii riippumattomana fyysisestä laitealustasta. Virtualisoitu käyttöjärjestelmä näkee, fyysisestä laitteesta riippumatta, aina samanlaiset fyysiset resurssit. Käyttöjärjestelmä näkee myös median, jolla virtuaalisovellus sijaitsee. Tosin se näkee sen fyysisenä kovalevynä, eikä esimerkiksi muistitikkuna tai Flash–muistina. (Löytömäki 2008).

Flash–muistille tai muistitikulle asennettava käyttöjärjestelmä ei itse asiassa ole mikään uusi keksintö. Esimerkiksi muistitikulle voidaan asentaa suoraan Windows XP-käyttöjärjestelmä, joka käynnistyy normaaliin tapaan. Myös vastaavia Linux–jakeluita on jo olemassa. Erona virtualisoidun, muistitikulla sijaitsevan käyttöjärjestelmän ja tavallisen käyttöjärjestelmän erona on laitteistoriippumattomuus ja riippumattomuus erilaisista ajureista. Virtualisointialusta mahdollistaa tuon riippumattomuuden. (Löytömäki 2008).

Tikuxin avulla työympäristö on aina mukana ja se toimii missä tahansa PC- tai Mac-tietokoneessa myös ilman internetyhteyttä. Kannettava tietokone on yksi mobiilin työympäristön käyttöön, mutta sen kantaminen ja mobiilisuus ei vastaa muistitikun ominaisuuksia. Muistitikulla oleva työympäristö takaa sen, että ympäristö on aina saatavilla, jos sitä sattuu tarvitsemaan ja isäntätietokone on saatavilla. Kannettavaa tietokonetta ei välttämättä tule ottaneeksi aina mukaan, kun poistuu toimistolta. Muistitikku kulkee helposti mukana esimerkiksi avaimenperänä. (Löytömäki 2008).

Tikuxin hyötykäyttö ei rajoitu pelkästään mobiilikäyttöön. Sitä voidaan hyödyntää myös organisaatioissa. Flash–muistitikku voi korvata fyysisen tietokoneen kovalevyn. Flash–muisti ei sisällä mekaanisia osia, kuten kovalevy, joten sen toimintavarmuus on huomattavasti suurempi kuin perinteisten kovalevyjen toimintavarmuus. Koska Flash–muisteissa ei ole mekaanisia osia, kuten magneettikiekon lukupäitä, on hakuaika huomattavasti nopeampi, varmatoimisempi ja tallennusmedian koko on huomattavasti pienempi. Muistitikut ovat myös äänettömiä. (Löytömäki 2008).

Organisaatiot itse ovat arvioineet, että tietokoneen käyttöikä on noin neljä vuotta. Käyttöiän arvio riippuu organisaatiosta. Itse kovalevyn käyttöikää on vaikea arvioida, koska ympäristötekijöillä on suuri vaikutus kovalevyn rasitemäärään. Esimerkiksi ilman lämpötila, pöly ja liike vaikuttavat mekaanisten osien kulumiseen ja toimintaan.

Tietokoneen kovalevyn rikkoontuessa työympäristöissä on edessä yleensä uuden koneen uudelleen asennus. Tikuxia käyttäessä voidaan työasema tai palvelinkone vaihtaa helposti. Siirretään vain muistimedia uudelle tietokoneelle ja käynnistetään virtualisoitu käyttöjärjestelmä. Virtuaalisovellus sisältää yleiset tai universaalit ajurit, jotka eivät ole riippuvaisia käytetystä fyysisestä koneesta. Yksi image-tiedosto muistitikulla, jolla käyttöjärjestelmä sijaitsee, on myös helposti varmuuskopioitavissa. Tuo tiedosto sisältää kaiken, mitä käyttöjärjestelmään liittyy, jolloin käyttäjän ei tarvitse miettiä tai pohtia mitä varmuuskopioidaan. Koko tietokone voidaan varmuuskopioida kopioimalla tuo yksi image-tiedosto. (Löytömäki 2008).

3.1 Tikuxin Tietoturva

Tikuxin maksullisessa Pro–versiossa virtualisoitu käyttöjärjestelmä, joka on siis yksi tiedosto muistitikulla, voidaan salata Advanced Encryption Standard (AES) –menetelmällä. Käytännössä tämä tarkoittaa perinteistä salasanaan turvautuvaa suojausta. Ilman oikeaa salasanaa, ei massamuistista saada mitään tietoja ulos. Pro–versiossa on myös oma palomuuri virtuaalialustassa, joka turvaa käyttöjärjestelmän verkosta tapahtuvilta hyökkäyksiltä. Palomuuri voidaan ottaa myös pois päältä, jolloin voidaan käyttää käyttöjärjestelmän omaa palomuurisovellusta. (Löytömäki 2008).

3.2 Player ja Tikux

Lähetin maaliskuussa 2008 Mikko Löytömäelle sähköpostilla jatkokysymyksenä oman tutkimuskysymykseni. Ottaen huomioon Tikux-tuotteen ominaisuudet ja salausmenetelmät, ei kyseistä ongelmaa ole ratkaistu ainakaan DRM-menetelmiä käyttäen. Toisaalta tuote eroaa hieman Player-sovelluksesta, koska se on rakennettu Linux:in pohjalta, kun taas WMware Virtual Player on puhtaasti Windows x86-tuote.

Findhill Oy on lähtenyt liikkeelle nimenomaan virtualisointiratkaisun kehittämisestä. Mikko Löytömäen vastauksista ja Tikux-tuotteen ratkaisuista jää päällimmäisenä tunne, että Tikux tuotteena on itse asiassa vain virtualisointiratkaisun sivutuote tai beta-testaajia varten räätälöity virtualisointiratkaisun kokeiluversio.

Miten voidaan suojata virtuaalikone kopioimiselta? Kryptaus perinteisenä suojausmetodina ei teorian ja käytännön valossa näytä kovin hyvältä vaihtoehdolta. Esimerkiksi pelkästään Windows XP -käyttöjärjestelmää tai muita vastaavia sovelluksia, jotka ovat suojattu tunnusavaimella, on varmasti jaettu vertaisverkossa tuhansia kappaleita. Business Software Alliancen (2008) mukaan suomessa joka neljäs ohjelmisto on laiton. Koko maailman ohjelmistoista 38 prosenttia on laittomia piraatteja. (BSA 2008).

Onko kryptaus siis tämän tiedon valossa sopiva suojausmenetelmä? Osaavissa käsissä ja oikeilla tiedoilla, mikään suojaus ei ole murtamaton ja se tarkoittaa kaikkia suojausmenetelmiä palomuureista RSA-tunnisteisiin. RSA-suojaukset ovat erittäin tehokkaita ja erittäin yleisesti käytettyjä ratkaisuita VPN-yhteyksien suojaamiseen. DRM-suojaukset eivät myöskään ole murtamattomia. Suojausten yleinen idea on kuitenkin tehdä murrot ja väärinkäytökset tavalliselle henkilölle erittäin vaikeaksi.

Jos tietojen suojaukseen ja yrityksen tietoturvaan perehtyy enemmän, sekä yrittää hahmottaa tietoturvaan rajoja, päästään vastaukseen, joka tarjoaa tarpeeksi suojaa ja turvaa arkaluontoisiin tietoihin. Suojaus itsessään on vasta ensimmäinen keino turvata tietoja. Käyttäjien kouluttaminen, ohjeistukset ja säännöt ovat vähintäänkin yhtä tärkeitä välineitä tietoturvaan liittyvissä asioissa. Esimerkiksi kryptaus tarjoaa suojaa, mutta katsooko yritys sen olevan riittävä suojaus?

Moderni informaatio- ja kommunikaatioyhteiskunta turvautuu yhä enemmän tietoteknisiin ratkaisuihin, sekä julkisella että yksityisellä sektorilla. Monet prosessit ovat elektronisesti ohjattuja ja sisältävät suuren määrän tietoa, jota lähetetään eteenpäin tietoverkkojen välityksellä. Suurin osa tehtävistä organisaatioissa ei enää olisi edes mahdollista ilman tietotekni-

siä järjestelmiä. Tosin riippuvaisuus tietojärjestelmistä vaihtelee työtehtävien välillä. Melkein kaikki organisaatiot kuitenkin ovat riippuvaisia toimivasta tietojärjestelmä infrastruktuuristaan. Organisaatiot voivat saavuttaa tavoitteensa vain jos tietojärjestelmän toimivuus on aina taattu. (BSI 2004).

Tietotuva kuvataan yleisesti tiedon käytettävyydellä, luottamuksellisuudella ja eheydellä. Käytettävyydellä tarkoitetaan sitä, että tiedon tulee olla saatavilla aina kun sitä tarvitaan. Luottamuksellisuudella tarkoitetaan, että tietoon pääsee käsiksi ainoastaan siihen oikeutetut henkilöt. Eheydellä tarkoitetaan tiedon oikeellisuutta. Tieto on juuri se tieto, joka sen kuuluu olla, eikä sitä ole muutettu ulkopuolisen henkilön toimesta, tai tieto ei ole korruptoitunut. (BSI 2004).

Organisaatioiden tietoturva on perusedellytys tietojärjestelmien toimivuudelle. Saksan tieturvavirasto, Bundesamt für Sicherheit in der Informationstechnik eli BSI, on tehnyt kattavan tietoturvaohjeistuksen julkiseen käyttöön. Sitä käytetään laajalti ympäri maailmaa organisaatioissa kartoittamaan tietoturvapolitiikkaa. Se tarjoaa kaikille organisaatioille ohjeistuksen, jolla organisaatiot voivat saavuttaa itselleen riittävän tason tietoturvassa. Manuaalissa luetellaan kattava lista erilaisista tietoturvauhkista, sekä ratkaisut uhkien minimoimiseksi.

BSI:n tietoturvamanuaalissa käsitellään kohdassa 5.4 uhkakuvaa varkaudesta. Laitteiston, välineiden, sovellusten tai tiedon varkaus johtaa rahallisen menetyksen lisäksi käytettävyyden ja luottamuksellisuuden menetykseen. Varkauden tapahtuessa, esimerkiksi laitteiston kohdalla ei voida varmuudella tietää, saako kukaan luvattomasti luottamuksellista tietoa laitteiston sisältä haltuunsa. Myöskään ei voida aina tietää, pääseekö laitteistolla käsiksi esimerkiksi yrityksen verkon kautta erilaisiin järjestelmiin. (BSI 2004). Manuaalissa käsitellään varkaustapausten minimoimiseksi lähinnä erilaisia käyttäjän huolellisuuteen liittyviä ratkaisuja. Laitteita ei tulisi jättää ilman valvontaa tai avoimesti esille julkisilla paikoilla.

BSI-manuaalin Safeguard kohdassa S 4.30 (BSI 2004) esitetään ratkaisuja sovellusten turvaratkaisuihin. Ratkaisuissa esitellään tekniikkaa, jossa sovelluksen avaamisen yhteydessä kysytään salasanaa. Tällä pyritään estämään sovelluksen luvaton käyttö. Sovelluksen sisällä voidaan käyttää ratkaisua, jossa pyydetään salasanaa operoidakseen sen kautta käsiteltävää tietoa. Esimerkiksi tiedon avaamisen yhteydessä pyydetään salasana, jolla päästään käsiksi tietoon. (BSI 2004).

Ottaen huomioon tutkimusongelman laadun, BSI-manuaalin antama ohjeistus ei välttämättä tarjoa vielä ratkaisua turvalliseen virtualisoituun, mobiiliin käyttöjärjestelmään. Varkaus koetaan selkeänä uhkana, mutta sen ratkaisemiseksi ei anneta eliminoivia ratkaisuja tai ohjeita.

Opinnäyteytössäni pyritään antamaan myös ratkaisu, joka täyttäisi vaatimukset myös BSI-manuaalin ohjeistuksen puitteissa yrityksen näkökulmasta.

Mikko Vestola toteaa tietotekniikkaoikeuden seminaarityönsä johtopäätöksessä (2007), että tehokkaan suojauskeinon määritteleminen on hankalaa, eikä tehokkaalle tekniselle suojakeinolle ei ole olemassa yksiselitteistä tulkintaa. Tehokkaan teknisen suojakeinon tulkinta riippuu paljon siitä, keneltä asiaa kysyy. Esimerkiksi kuluttajien ja tekijänoikeusjärjestöjen intressit ovat hyvin erilaisia ja käsitykset yleensä poikkeavat tässä toisistaan. (Vestola, 2007).

4 Tulokset

Perustuen tutkimiini DRM–teknologioihin PDF–tiedostojen sekä Windows Rights Management –palvelun osalta virtuaalisen koneen tulisi pystyä suojaamaan sovelletusti molemmilla tekniikoilla.

Virtuaalikoneen image–tiedosto suojataan laitetunnuksen perusteella. Lisäksi tuohon tiedostoon lisätään lisensointikoodi, joka viittaa RMS-palvelimeen, johon on pääsy julkisesta internetyhteydestä. Avatessani virtuaalikoneeni tarkistaa virtuaalisovellus oikeuteni virtuaalikoneeseeni RMS–palvelimelta muistitikun laitetunnuksen perusteella. Mikäli oikeudet ovat kunnossa kriteereiden osalta, saan virtuaalikoneeni auki.

Tutkimuskysymykseni on ollut: ”Mistä tiedän onko virtuaalikoneeni varastettu?”. Tuon yksittäisen image-tiedoston kopioiminen on yhtä helppoa kuin tavallisenkin tiedoston. Mikäli imagetiedostoni olisi kopioitu ja se yritetään avata jossain muussa muistitikussa kuin RMS–palvelimelle rekisteröidyn lisenssitiedon perusteella, jäädyttää RMS–palvelin kaikki oikeudet tuohon image-tiedostoon. Kopioidun virtuaalisen koneen image-tiedoston lisenssitietoon rekisteröity laitetunnus ei vastaa RMS–palvelimelle rekisteröityä tietoa.

Väärinkäytön yhteydessä kaikkien versioiden sekä kopioidun että alkuperäisen virtuaalikoneen avaamisessa tapahtuva oikeuksien kysely RMS-palvelimelta epäonnistuu. Tässä tilanteessa RMS-palvelin ilmoittaa paluuviestinä virtuaalikoneeni varastetuksi ja kaikki oikeudet virtuaalikoneen käyttöön evätään.

5 Johtopäätökset

Monissa tapauksissa perinteinen salasana suojaus tai muistitikun kryptaus ei ole riittävä tapa suojata virtuaalikonetta. Mielestäni työympäristössä, jossa saatavilla on paljon arkaluontoiseksi luokiteltavaa tietoa, tulee suojata tietokoneet ja itse tieto parhaalla mahdollisella tavalla. Olen tullut johtopäätökseen, että DRM-teknologiaan perustuva suojaus on ainoa var-

teenotettava vaihtoehto, jos työkoneeni on virtuaalinen tietokone muistitikulla tai vastaavalla medialla ja se halutaan suojata parhaalla mahdollisella tavalla.

Kryptaus perinteisenä menetelmänä ei anna vastausta tutkimusongelmana esitettyyn kysymykseen. Tutkimuksessa esitetty ratkaisu DRM-teknologian osalta tuo ratkaisun sillä varauksella, että valmista tai kaupallista ratkaisua ei ole tarjolla nykyisillä markkinoilla. Nykyiset DRM-suojaukset ovat olleet helposti kierrettävissä esimerkiksi CD-levyissä käyttäen CD:n polttamiseen tai konvertoimiseen erillistä sovellusta. (Järvinen 2006). Tämä koskee siis DRM:llä suojattuja CD-levyjä ja musiikkia sisältäviä mp3-tiedostoja.

DRM-suojatun virtuaalikoneen turvallisuutta ei voida käytännössä todistaa, koska virtuaalikoneille ei ole tarjolla kaupallista DRM-ratkaisua. Jos tilannetta tarkastellaan nyt käytössä olevia ratkaisuja, ne eivät tarjoa riittävää turvallisuutta.

Opinnäytetyössäni käsiteltyä ilmiötä ei tavallisen, yksityisen käyttäjän näkökulmasta pidetä tietoturvariskinä. Virtualisointisovelluksen sulkeminen ja käyttöjärjestelmän sulkeminen nukkumistilaan on sovelluksen yksi ominaisuus, eikä varsinaisesti tietoturvariski. Riski tietoturvassa kasvaa, riippuen siitä mitä virtualisoidulla käyttöjärjestelmällä tehdään ja mihin tietoihin sillä voi päästä käsiksi.

Jos virtualisoitu käyttöjärjestelmä sisältää pelkästään itse käyttöjärjestelmän ja varmuuskopioina kuvia viimeiseltä kesälomalta, varkauden sattuessa menetys ei välttämättä tuota muuta kuin harmia menetyksen uhrille. Jos se sisältää pääsyn henkilökohtaiseen sähköpostiin ja kopion mahdollisesti keskeneräisestä opinnäytetyöstä, on menetys jo mitattavissa esimerkiksi menetetyillä työtunneilla, joita kirjoittamiseen on käytetty.

Tutkimukseni vastaa tarpeeseen suojata virtualisoitu, mobiili käyttöjärjestelmä parhaalla mahdollisella tavalla. Tavallinen kryptaus voi olla riittävä, mutta se ei välttämättä tuo parasta mahdollista suojaa luottamuksellisille tiedoille. Yksityinen henkilö voi katsoa kryptauksen tai drm-suojauksen tarpeettomaksi kokonaan. Muistitikku avainnippuun kiinnitettynä ja jatkuvasti kuljetettuna housuntaskussa voi olla jo tarvittava suojausmetodi. Tarpeeksi kattavan suojausmetodin pohtii aina käyttäjä itse.

Monilla organisaatioilla tietojärjestelmien toimivuudesta riippuu koko organisaation taloudellinen menestyminen. Tämä tarkoittaa myös sitä, että yksittäisen työntekijän mahdollisuus suoriutua työstään riippuu tietojärjestelmän toimivuudesta. Yritysten ulkopuolella ihminen on myös riippuvainen erilaisten järjestelmien toimivuudesta. Puhelimet, televisio, julkinen liikenne, sekä esimerkiksi pankkikorttien käyttö maksuvälineenä ovat täysin riippuvaisia toimivasta tietojärjestelmästä. Kun yhteiskunta on jatkuvasti yhä enemmän riippuvainen tietojär-

jestelmistä, riskit järjestelmien kaatumiseen ja sen seurauksena tapahtuviin vahinkoihin lisääntyvät. Mikään tietojärjestelmä ei ole riskitön, eikä ilman heikkouksia. Tämän johdosta yleisesti kiinnostus ja panostaminen tietoturvaan on kasvanut.

Yritysmaailmassa tietoturvapolitiikka määrittelee organisaation perustason tietoturvan ja sen ratkaisuiden suhteen. Yritykset voivat käyttää hyödyksi esimerkiksi BSI–manuaalia kartoittaakseen omat tarpeensa ja puutteensa tietoturvan suhteen. Käytännön tietoturvaratkaisut ja perustaso tietoturvassa luodaan juuri tietoturvapolitiikan ja ohjeistuksen perusteella. Perusteellisella kartoituksella ja tietoturvapolitiikalla organisaatio minimoi riskit käytettävyyden, eheyden ja luottamuksellisuuden suhteen jokaisella osa-alueella.

Yksi tiedosto muistitikulla, joka on teknisesti jokaisen kopioitavissa ja käytettävissä rikkoo tietoturvan peruskäsitteisiin liittyvän säännön. Kopioitavissa oleva ja ilman autentikointia avautuva käyttöjärjestelmä ei täytä luottamuksellisuuden sääntöä. Yleisesti ratkaisu autentikointiin ja pääsy tietoon on suojata se salasanalla käyttäen kryptausteknologioita.

Opinnäytetyössäni on käsitelty samaa ongelmaa eri näkökulmasta. Suojatulla tiedolla ei tee mitään ja suojatun tiedon suojaus väärinkäytöksen tapahtuessa sulkee kaiken pääsyn tietoon itseensä. Sillä voidaan taata tiedon luottamuksellisuus ainakin tiettyyn pisteeseen asti.

Keskusteluissani yleisesti eri IT-asiantuntijoiden kanssa, yleisellä tasolla kaikkien henkilöiden mielipide suojausten pitävyydestä ja luotettavuudesta on ollut lähes sama. Osaavissa käsissä mikään suojaus ei ole läpäisemätön. Esimerkiksi palomuurien suojauksissa jo yksi avonainen portti voi olla tarpeeksi, jos verkkomurtoa tekee osaava henkilö. Sama perusperiaate liittyy kaikkiin suojausmetodeihin. Teoreettisella tasolla, minkä tahansa suojauksen pystyy purkamaan. Kysymyksenä tietoturva asioissa onkin se, minkä suojausmetodin ja tietoturvaratkaisun katsotaan olevan riittävä organisaation näkökulmasta. Riittävällä tarkoitetaan tasoa, jossa rajataan riskit mahdollisimman pieniksi.

VMware Player –sovelluksen ”hibernate” ominaisuuden organisaatio voi katsoa jopa ratkaisevaksi tekijäksi ylipäätään sen käytön mahdollisuudesta yrityksessä. Tietoturvapolitiikan perusteella organisaatio voi kokea, että sen tuoma riski on liian suuri yritykselle ja sen tietojen luottamuksellisuudelle, vaikka se voitaisiinkin suojata joko kryptauksella tai DRM–suojauksella. DRM–suojaus kuitenkin takaa luottamuksellisuuden huomattavasti eri tavalla, kuin perinteinen kryptausteknologia. Juuri DRM–suojauksen erilaiset ominaisuudet ja käyttömahdollisuudet tekevät siitä mielenkiintoisen.

6 Yhteenveto

Tämä opinnäytetyö on esimerkki todellisen elämän tietoteknisestä ongelmasta. Työ yrityksen teknisessä hallinnossa ja erilaisissa tukitehtävissä on juuri tämän kaltaisten ongelmien ratkaisua. Jos ajatellaan tukitehtäviä ja teknistä hallinnointia organisaatiossa filosofisella tasolla, on aihe vielä mielenkiintoisempi.

IT–osaston funktio organisaatiossa on tukea yrityksen toimintaa. Filosofisella tasolla informaatioteknologian, IT–osaston ja tukitoimintojen tehtävä on helpottaa yrityksen työntekijöiden tehtäviä. Omasta mielestäni päämäärä tietojärjestelmissä ja esimerkiksi palvelinten osalta on saada niiden tekemät tehtävät automaattisiksi. Korttipalvelimet ovat yksi esimerkki uusista palvelinratkaisuista, joiden toiminta virtualisoinnin myötä voidaan automatisoida.

Esimerkiksi automatisoidun palvelimen rikkoontuessa, automatisoitu robotti vaihtaa uuden palvelinkortin kehikkoon, eikä katkoksia synny. Rikkoontuminen ei myöskään tuo IT–tuelle ylimääräistä työtä. IT-osasto joutuu työnä tilaamaan uuden varapalvelinkortin laitetoimittajalta. Mielestäni tällaiseen tilanteeseen tulee kaikkien IT–järjestelmien ja IT–osastoiden pyrkiä. Tekninen suorittaminen työtehtävissä ei tuo organisaatiolle kehitysinnovaatioita yrityksen sisältä, koska luovalle ajattelulle ei jää tarpeeksi siihen vaadittua aikaa.

IT–osaston perimmäinen tarkoitus on myös kehittää yrityksen tietojärjestelmiä. Ilman luovaa ilmapiiriä yritys itse ei välttämättä tuota uusia ideoita järjestelmien kehittämiseksi. Usein ulkopuoliset konsultit näkevät asioita, joita yrityksen IT–henkilöstö ei näe itse. Vasta ulkoinen havainnointi tuo ahaa–elämyksen.

Olen oman tutkimusongelmassani pyrkinyt ideoimaan ratkaisua virtualisointisovelluksen tietoturvan parantamiseksi. Olen myös asettanut itselleni tavoitteen kehittää omaa luovaa ajatteluani. Ottaen huomioon filosofiset seikat voi DRM–teknologiaa hyödyntää teoreettisesti myös muilla osa-alueilla suojausmenetelmänä.

Työntekijöiden autentikointi järjestelmiin voidaan automatisoida, jolloin se tapahtuu työntekijälle läpinäkyvästi. Työntekijä ei itse tiedä, millä kriteerillä hänet autentikoidaan yrityksen verkkoon tai järjestelmiin. Työntekijän ei esimerkiksi itse tarvitse tietää viittä eri salasanaa eri järjestelmiin, koska autentikointi tapahtuu muulla tavalla kuin perinteisesti salasanaa hyödyntävällä autentikoinnilla. Tämä ajatus tukee IT–yksikön filosofista tarkoitusta organisaatiossa, joka pyrkii automatisoimaan tietojärjestelmänsä tukeakseen yrityksen liiketoimintaa parhaalla mahdollisella tavalla.

Lähteet

Apple, 2008. iTunes ja iPod sivusto. [www-sivusto] http://www.apple.com/fi/itunes/ (haettu 10.10.2008).

Business Software Alliance. 2008. BSA: Laittomien Ohjelmistojen Käyttö Vähentynyt Suomessa. [www-sivusto] http://w3.bsa.org/finland/press/newsreleases/BSA-LAITTOMIEN-OHJELMISTOJEN-KAYTTO-VAHENTYNYT-SUOMESSA.cfm (haettu 23.11.2008).

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2004. IT Grundschutz Manual. [e-kirja] http://www.bsi.bund.de/english/gshb/manual/index.htm (haettu 15.04.2008).

Coyle, C. 2003. The Technology of Rights: Digital Rights Management. Talk given at the Library of Congress on November 19th 2003. http://www.kcoyle.net/drm_basics1.html (tulostettu 15.03.2008).

Electronic Frontier Finland ry. 2008. Lyhennesanasto [www-sivusto] http://www.effi.org/yhdistys/sanasto.html (haettu 12.10.2008).

Eran, D. 2006. Hacking iPod Games: How Apple's DRM Works. [www-artikkeli] http://www.roughlydrafted.com/RD/Home/728B5C4B-0A35-40BE-A2E7-E5464C68B80A.html (luettu 10.10.2008).

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. 13. painos. Keuruu: Otavan Kirjapaino Oy.

Järvinen, A. & Järvinen, P. 2004. Tutkimustyön Metodeista. Tampere: Tampereen Yliopistopaino Oy.

Järvinen, P. 2006. Näin Murtuu Kopiosuojaus. Tietokone –lehti 01/06 [online] http://www.tietokone.fi/lukusali/artikkelit/2006tk01/kopiosuojaus.htm (luettu 23.11.2008).

Koski, J.T., Tuominen, S. & Kärkkäinen, I. 2007. Kuinka ideat syntyvät. Porvoo: WS Bookwell Oy.

Kurri, S. 2008. Käyttöjärjestelmä kulkee USB-muistilla suomalaisvoimin. Muropaketti.com 18.03.2008. http://plaza.fi/muropaketti/kayttojarjestelma-kulkee-usb-muistilla-suomalaisvoimin (luettu 18.03.2008).

Laudon, K. & Laudon J. 2006. Management Information Systems: Managing The Digital Firm. 9. painos. Pearson Education, Inc.

Layton, J. 2006. How Digital Rights Management Works. [www-artikkeli] http://electronics.howstuffworks.com/drm.htm (haettu 15.03.2008).

Löytömäki, M. 2008. Findhill Oy : Tikux. Säköpostikeskustelu 03.04.2008 mikko.loytomaki@findhill.com. Tulostettu 04.04.2008.

Microsoft Corporation. 2005. Microsoft Windows Rights Management Services for Windows Server 2003 : Helping Organizations Safeguard Digital Information from Unauthorized Use. [word-dokumentti] http://download.microsoft.com/download/b/f/4/bf49f1b6-554a-4f6c-8272-2efc782dcd1c/RMSHelpsSafeguard.doc (haettu 16.03.2008).

Motion Picture Association of America. 2005. 2005 U.S. Piracy Fact Sheet. [PDF-dokumentti] < http://www.mpaa.org/USPiracyFactSheet.pdf> (tulostettu 15.03.2008).

Vestola, M. 2007. Mikä on "tehokas" tekninen suojakeino?. Seminaarityö. [PDF] http://www.mvnet.fi/index.php?osio=Tutkielmat&luokka=Yliopisto&sivu=Mik%E4_on_tehokas_tekninen_suojakeino&tyyppi=PDF (haettu 10.10.2008).

Getting Started Guide: VMware Player 2.0. 2007. VMware, INC.[PDF-dokumentti] http://www.vmware.com/pdf/vmware_player200.pdf (tulostettu 25.01.2008).

Transparent Paravirtualization. 2008. VMware, Inc. [www-sivusto] http://www.vmware.com/interfaces/paravirtualization.html (haettu 26.10.2008).

Understanding Full Virtualization, Paravirtualization, and Hardware Assist. 2007. VMware, INC. [PDF-dokumentti] < http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf> (tulostettu 16.02.2008).

Virtualization Basics. 2008. VMware, INC. [www-sivusto] http://www.vmware.com/virtualization/ (haettu 26.10.2008).

Virtualization Overview (VMware White Paper). 2006. VMware, Inc. [PDF-dokumentti]. http://www.vmware.com/pdf/virtualization.pdf (tulostettu 16.02.2008).

VMware VMotion. 2008. VMware, Inc. [www-sivusto] http://www.vmware.com/products/vi/vc/vmotion.html (haettu 26.10.2008).

Liitteet