hyväksymispäivä arvosana

arvostelija

Digitaalisten oikeuksien hallinta yhteistyöverkostoissa

Laura Markova

Helsinki 06.04.2012

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET

Tiedekunta/Osasto	Laitos – Institution
Matemaattis-luonnontieteellinen	Tietojenkäsittelytieteen laitos

Tekijä – Författare
Laura Markova

Työn nimi – Arbetets titel
Digitaalisten oikeuksien hallinta yhteistyöverkostoissa

Oppiaine – Läroämne
Tietojenkäsittelytiede

Työn laji – Arbetets art	Aika – Datum	Sivumäärä – Sidoantal
Pro gradu -tutkimussuunnitelma	06.04.2012	24 sivua

Tiivistelmä – Referat

Tämän Pro gradu –tutkielman aihe on DRM eli digitaalisten oikeuksien hallinta, tarkemmin omistajuuden jäljitettävyys. Työ on vertaileva kirjallisuuskatsaus (survey) yhteistyöverkostojen käyttöön sopivista DRM-tekniikoista. Tutkielma pyrkii vastaamaan kysymykseen, millaisia eri tekniikoita on olemassa digitaalisen sisällön oikeuksien hallintaan, ja mikä tai mitkä niistä soveltuvat parhaiten erilaisiin yhteistyöverkostoihin.

ACM Computing Classification System (CCS):
E.3 [DATA ENCRYPTION]: Public key cryptosystems, Standards
K.4.1 [Public Policy Issues]: Intellectual property rights, Privacy
K.4.3 [Organizational Impacts]: Computer-supported collaborative work
K.4.4 [Electronic Commerce] :Intellectual property
K.5.1 [Hardware/Software Protection]: Copyrights, Licensing, Proprietary rights
K.6.5 [Security and Protection]: Authentication

Avainsanat – Nyckelord
DRM, digitaalinen oikeuksien hallinta, omistajuuden jäljitettävyys, yhteistyöverkostot, yksityisyyden suoja

Säilytyspaikka – Förvaringställe
Kumpulan tiedekirjasto, sarjanumero C-2004-

Muita tietoja – Övriga uppgifter

Sisältö

1 Johdanto

Digitaalisten oikeuksien hallinta (DRM, Digital Rights Management) on yhä tärkeämpää modernissa yhteiskunnassamme. Tietotekniikan, tietoliikenteen ja kommunikaation, kuluttajaelektroniikan sekä näiden yhdistelmien tuottama digitaalisen sisällön määrä kasvaa kiihtyvään tahtiin, ja on tuonut mukanaan kysymyksiä sisällön luojan, tuottajan ja jakelijan oikeuksista ja velvollisuuksista, sekä myös tuotteen käyttäjän oikeuksista ja velvollisuuksista.

Digitaalisten oikeuksien hallinnalla viitataan laajasti ryhmään käytäntöjä, tekniikoita ja työkaluja, jotka ohjaavat oikeanlaiseen digitaalisen sisällön käyttöön [SuB06]. DRM-järjestelmän avulla sisällön luoja voi määritellä mitä käyttöoikeuksia muut voivat saada sisällölle. Sisällön tuottaja pystyy luomaan sisällöstä metatietoa ja määrittelemään puolestaan tuottajan oikeudet, jakelija valvomaan sisällön käyttöä ja seuraamaan maksuliikennettä. Sisällön käyttäjä puolestaan voi valita haluamansa sisällön ja sille jonkin tarjolla olevista käyttötapavaihtoehdoista.

Digitaaliset tekijänoikeudet ovat olleet uutisissa lähinnä piratismin, kuten musiikin tai elokuvien laittoman jakelun myötä. Analogisesti talletettu sisältö heikkeni jokaisen kopiointikerran myötä, mikä samalla automaattisesti suojeli sitä laittomalta jakelulta. Digitaalista kopiota ei käytännössä pysty laadun suhteen erottamaan alkuperäisestä, joten tämä suoja hävisi, ja luvaton jakelu, yleensä vertaisverkkojen kautta, lisääntyi sen myötä huomattavasti [DoK08]. Tämä toi kaupallisia tappioita digitaalisen sisällön omistajille.

Pilvipalveluiden lisääntyessä ja teknologian muuttuessa yhä avoimemmaksi, myös resurssien käytön hallinnan haasteet lisääntyvät. Toiset henkilöt ovat vastuussa sisällönhallinnasta, toiset systeemeistä joissa niitä säilytetään. Erilaiset laitteistot pienistä käsipäätteistä isoihin palvelimiin, resurssien liikkuminen kansallisten tai alueellisten rajojen ylitse, valmiiden algoritmien ohjaama tiedonsiirto, joihin käyttäjällä ei ole mitään sananvaltaa. Kaikki tämä vaatii uudenlaista käytönhallintaa [LJB11]. Nykyinen tämän alan tutkimus on keskittynyt parempien käyttöoikeuskielien kehittelyyn joko matemaattisen logiikan tai suurempaa päättelykykyä omaavan formalismin kautta, eikä vastaa

suurimpaan käytännön haasteeseen, joka on digitaalisen sisällön ja sen oikeuksienhallinnan yhteentoimivuus erilaisten järjestelmien välillä.

Yksi tärkeä näkökanta digitaaliseen oikeuksien hallintaan ovat tiedon salassapitoon liittyvät kysymykset: tietyn ryhmän hallussa olevan tiedon ja digitaalisen sisällön leviäminen ryhmän ulkopuolelle tulisi estää, myös ryhmän hajoamisen jälkeen. Salassapidettävän tiedon päätyminen vääriin käsiin voi tuoda laitonta kilpailuetua, tai ääritapauksissa jopa vaarantaa turvallisuutta. Tieteellisissä yhteisöissä tiedon hallittu jakaminen ja keskustelevat yhteistyöverkostot ovat arkipäivää. Nykyisin myös yritysten pitäisi tehdä syvempää ja laajempaa yhteistyötä menestyäkseen, luoda omia kontaktiverkostojaan eri suuntiin. Näissä verkostoissa on tärkeää rajata ja hallita jaetun ja toisaalta muiden seurassa salassapidettävän digitaalisen tiedon rajat: kontrolloida laillista informaatiovirtaa, ja huomata ajoissa laittomat informaatiovirrat. Myös yksityisyyden kunnioittamiseen liittyvät kysymykset nousevat silloin pakostakin esille.

Tämän pro gradu –tutkielman aihe on DRM eli digitaalisten oikeuksien hallinta, tarkemmin rajattuna omistajuuden jäljitettävyys. Tutkielma on vertaileva kirjallisuuskatsaus (survey) yhteistyöverkostojen käyttöön sopivista DRM-tekniikoista. Se pyrkii vastaamaan kysymykseen, millaisia eri tekniikoita on olemassa digitaalisen sisällön oikeuksien hallintaan, ja mikä tai mitkä niistä soveltuvat erilaisiin yhteistyöverkostoihin.

Tutkielman tuloksena nähdään että...

Tutkielman luvussa 2 määritellään ja kuvataan tarkemmin mitä DRM on. Siinä etsitään vastauksia kysymyksiin, ketkä tarvitsevat DRM-tekniikoita, mihin niitä tarvitaan ja miksi. Myös digitaalisen sisällön elinkaarta mietitään, lähinnä sen kautta, minkälaista suojaa tieto missäkin vaiheessa elinkaartaan tarvitsee. Luvussa 3 esitellään erilaisia DRM-tekniikoita ja luokitellaan niitä niiden piirteiden perusteella. Karkeasti jaettuna eri DRM-tekniikat jakaantuvat käyttäjien valvontaan, itse sisällön merkitsemiseen tekijänoikeusmerkinnöin, tai petturin jäljittämiseen perustuviin tekniikoihin. Tarkoituksena on ryhmitellä

näihin ryhmiin kuuluvia eri tekniikoita niin yhteisten kun erottavienkin piirteiden perusteella. Luvussa 4 vertaillaan näitä eri DRM-tekniikoita sen perusteella, kuinka hyvin ne soveltuvat yhteistyöverkostoissa jaettavan digitaalisen sisällön hallintaan. Viimeisessä luvussa 5 esitetään tämän tutkielman tulos, mitä ratkaisuja löydettiin ja mitä niistä voitiin päätellä. Yhteenvedossa pohditaan myös tutkielman tulosten vaikutusta aihealueeseen, ja esitellään mahdollisia jatkotutkimusaiheita.

2 Digitaalisten oikeuksien hallinta

Elämällämme teknologian aikakaudella on paljon erilaisia digitaalisia tallennuslaitteita. Niinpä myöskin suurin osa tiedosta ja sisällöstä on tallennettuna digitaaliseen muotoon. Digitaalisen tuotteen manipulointi, kopiointi ja uudelleen jakaminen on verrattain helppoa [ElA07]. Tämän teknologisen kehityksen mukanaan tuomaan tiedollisen omaisuuden ja digitaalisen median hyväksikäyttöön, sekä piratismin uhan kasvuun voidaan vastata kolmella aseella: teknologialla, lainsäädännöllä ja liiketoimintamalleilla [ETD03]. Tiedollinen omaisuus voidaan jakaa teolliseen omaisuuteen, jota suojellaan patentein ja tavaramerkein, ja tekijänoikeuksien alaisuuteen kuuluvaan omaisuuteen. Digitaalisen sisällön tekijänoikeuksista puhuttaessa puhutaan juuri DRM-tekniikoista.

Tekijänoikeuslain alainen digitaalinen sisältö kohtaa siis haasteen: laiton käyttö pitää estää, mutta haittaamatta laillisesti tuotetta käyttävän kuluttajan oikeutta käyttää hankkimaansa sisältöä, mahdollisesti eri välineiden kautta. Sisällönhallinnan säännöt ovat vielä osittain avoimia: miten digitaalista sisältöä käytetään yhdessä, ensinnäkin laillisesti, ja toisaalta kaikkien osapuolten hyväksymissä rajoissa, mahdollisimman monen tarpeet tyydyttäen?

Tiedon turvallinen jakaminen voidaan tarkasti määritellen erottaa DRM-tekniikoista, joiden pääasiallisena tarkoituksena voidaan nähdä olevan sisällön suojeleminen, jotta myyntituotot eivät häviäisi [SRZ06]. Turvallisen tiedon jakamisen tavoite on ”jakaa mutta suojella”, eli jakaa haluttu sisältö kaikkien sitä tarvitsevien käyttöön, mutta suojella arkaluonteista sisältöä luvattomalta paljastumiselta. Mitä helpommaksi jakaminen tulee, sitä vaikeammaksi

suojeleminen muuttuu. Luotettu tietojenkäsittely (trusted computing) tarjoaa joitain ratkaisuja tähän turvalliseen tiedonjaon ongelmaan.

Historiallisesti tiedon jakamiseen on ollut neljä erilaista lähestymistapaa: klassinen harkinnanvarainen käytön kontrollointi (DAC, discretionary access control), pakollinen käytön kontrollointi (MAC; mandatory access control), perustajan kontrolli (ORCON, originator control), ja nyt neljäntenä luotettu tietojenkäsittely [SRZ06].

Luotettu tietojenkäsittely korostuu esim. potilastietojen käsittelyssä, jossa terveystietojen tallentaminen pilvipalveluihin ja niiden elektronien haku eri verkostojen kautta on kasvava trendi [JSS11]. Näiden tietoturva ja yksityisyydensuoja ovat kriittisiä käsitteitä, koska terveystiedot ovat kaikkein yksityisimpiä yksilöistä talletettavia tietoja. Pilvipalveluiden hajautettu luonne, ja tietojen varastoinnin ja siirron altistuminen asiankuulumattomille herättävät erityishuolta tiedon salassapysymisestä. Tietoturvaan liittyvät epäilykset puolestaan kasvattavat riskiä siitä, tallennetaanko varmasti kaikki tarvittavat tiedot järjestelmiin, vai jäävätkö jotkin arkaluontoisemmat tiedot tallentamatta. Pilvessä olevien terveystietojen saatavuus vain luvallisille käyttäjille onkin tärkeä vaatimus. Potilaskeskeisessä lähestymistavassa potilaalla on päärooli hänen omien tietojensa luomisessa ja pääsynvalvonnan kontrolloinnissa. Potilas ei kuitenkaan saa muuttaa omia tietojaan, vaan ainoastaan kontrolloida sitä, minkä tahojen kanssa jokin tahon hänestä tallentamat tiedot voidaan jakaa.

Periaatteessa turvallinen tiedon jakaminen voidaan jakaa kahteen osioon: joko sallitaan tiedon kopiointi ja jakaminen, kunhan tieto on suojattu ainakin yhtä hyvin kuin originaali, tai halutaan estää tiedon kopioiminen kokonaan. Digitaalisella oikeuksien hallinnalla pyritään hallitsemaan sitä, kuka, miten ja missä pääsee käsiksi tietosisältöön. Digitaalisen sisällön elinkaaren aluksi tieto suojataan. Sisältöä eteenpäin jaettaessa sen käyttöä valvotaan, tietoa jaetaan eteenpäin hallitusti, sallituille käyttäjille tai käyttäjäryhmille. Digitaalisen sisällön elinkaaren loppupäässä tutkitaan, onko sisältöä käytetty sallitusti, vai onko sitä levitetty myös laittomasti. Jos on, pettureita rangaistaan ja mietitään miten estettäisiin saman toistuminen jatkossa.

2.1 Mitä DRM on?

DRM-järjestelmät koostuvat arkkitehtuureista, protokollista ja teknologioista joiden tarkoitus on luoda tyydyttäviä ratkaisuja digitaalisen sisällön oikeuksien hallinnan mukanaan tuomiin ongelmiin: laittoman käytön esto laillisen käytön hankaloitumatta liikaa, ja yksityisyyden suojaa loukkaamatta [ElA07]. Itse digitaalisen oikeuksien hallinnan eli DRM:n määrittely yksikäsitteisesti on hankalaa, sillä se voidaan määritellä joko lakien tai ekonomian, teknisen tai toiminnallisen puolensa kautta [Die08]. Tässä tutkielmassa digitaalisten oikeuksien hallinnalla viitataan laajasti ryhmään käytäntöjä, tekniikoita ja työkaluja, jotka ohjaavat oikeanlaiseen digitaalisen sisällön käyttöön [SuB06].

Digitaalisen sisällön laillisen ja tehokkaan käytön takaamisen lisäksi on huomioitava, että kuluttajan yksityisyyden suojaa ei tulisi loukata. DRM:n vaikutus käyttäjien yksityisyyteen on herättänyt kasvavaa levottomuutta [OwA04]. DRM-sovellus voidaan asettaa keräämään käyttötietoja aina kun käyttäjä koskee tiettyyn digitaaliseen sisältöön, joten potentiaali vakaviin yksityisyyden suojaan tunkeutumisiin on olemassa. Teknologia kehittyy jatkuvasti, ja samalla sen käyttö lisääntymistään lisääntyy yhteiskunnassamme. Teknologian käyttäjämäärien kasvaessa huikeaa tahtia, lisääntyvät myös nämä kysymykset digitaalisen sisällön luojan ja toisaalta sen ostaneen omistajan oikeuksista. Näiden vaatimusten välissä tasapainoilemisessa riittää vielä haastetta. DRM-järjestelmällä onkin tärkeä rooli monissa prosessin vaiheissa sisällön kulkiessa sen luojalta loppukäyttäjälle [SuB06].

DRM-järjestelmä hallinnoi sisällön oikeanlaista käyttöä. Sen avulla sisällön luojan raaka materiaali pakataan sopivaan muotoon, suojellaan sisältöä sen asiattomalta muokkaamiselta ja käyttämiseltä, ja määritellään mitä käyttöoikeuksia sisältöön voi hankkia. DRM-järjestelmän pitää pystyä jakelemaan sisältöä helposti vertaisverkkojen tai Internetin kautta, ottamaan vastaa ja valvomaan maksuliikennettä, ja määrittelemään sisällön ja sitä käyttävien laitteiden autenttisuus. Sen pitää monitoroida sisällön käyttöä ja varmistaa, että käyttö vastaa sille annettuja oikeuksia, ja käyttö ja maksut ovat yhteneväiset, sekä hallita turvallisuuden ja yksityisyyteen liittyvät asiat [SuB06]. Tähän päälle kun lisätään kaikenlainen personointi kaikkien osapuolien tahoilta, erilaisten järjestelmien kanssa yhteentoimivuus, sekä vielä itse järjestelmän

helppokäyttöinen ja luotettava toiminta, alkavat DRM-järjestelmälle asetettavat minimivaatimukset ollakin koossa. DRM-järjestelmän on lisäksi oltava toisaalta salattu, toisaalta toiminnaltaan ja vaihtoehdoiltaan läpinäkyvä, ja mielellään innovatiivinen ja parempi kuin muut vastaavat DRM-järjestelmät.

Monet eri lait ja käyttötavat kohtaavat DRM:n parissa. DRM:ssä on potentiaalia tehdä mahdolliseksi hyvälaatuisen sisällön saaminen useiden käyttäjien käyttöön luotettavasti ja turvallisesti avointen jakeluverkostojen kautta [OwA04]. On kuitenkin muistettava, että mikään DRM-tekniikka ei takaa täydellistä suojaa sisällölle, vaan on aina olemassa riski, että DRM-toimintojen ja -tekniikoiden ympäri kierretään jollain tavalla [SuB06]. Jos digitaalista oikeuksienhallintaa ajattelee vain teknologisena kysymyksenä, voidaan DRM:ää pitää epäonnistumisena: on vain ajan kysymys, milloin mikäkin DRM-ohjelmisto saadaan kierrettyä, yleensä parin vuoden sisällä niiden julkaisemisesta.

DRM:n onnistuminen tai epäonnistuminen on kuitenkin myös lakiin ja yhteiskuntaamme liittyvä kysymys. Tekijänoikeuslaki perustuu käytännössä siihen, että laiton kopiointi on kallista ja hankalaa [Boy11]. Jos muistitikullisen laiton kopiointi saadaan yhtä hankalaksi kuluttajalle kuin kokonaisen nidotun kirjan kopiointi, sen sisällön käytöstä maksaminen tuleekin luontevaksi osaksi sen helppoa käyttämistä. Juuri tähän DRM-järjestelmien pitäisi osua, jotta niistä tulisi tulevaisuuden menestystarina digitaalista sisältöä jaettaessa: helpottaa kuluttajaa saamaan käyttöönsä haluttu digitaalinen sisältö pientä maksua vastaan.

2.2 DRM-järjestelmän toimintaesimerkkejä

Yksi pääfilosofia DRM-järjestelmissä on itse sisällön ja toisaalta sisällön käytölle annettavien oikeuksien erillisyys [SuB06]. Itse sisältöä voidaan jakaa ja ladata vapaasti; sitä ei kuitenkaan voi käyttää ilman voimassa olevaa lisenssiä, johon on määritelty asianmukaiset oikeudet. Nämä oikeudet määrittelevät selkeästi, miten niihin liittyvää sisältöä saa käyttää tämä kuluttaja tällä laitteella.

Käyttöoikeuksia voi määritellä monen asian suhteen [SuB06]. Näitä ovat esimerkiksi

- erääntymispäivämäärä, joka määrittelee minkä päivämäärän jälkeen sisältöä ei enää voi käyttää,
- aloituspäivämäärä, jota ennen sisältöä ei voi käyttää,
- käyttöjakso eli yhteen sidotut aloitus- ja loppumispäivämäärä, jotka määrittelevät kuinka monena päivänä sisältöä saa käyttää aloituspäivämäärän jälkeen,
- soittokertojen määrä, kuinka monta kertaa sisältöä saa käyttää,
- laitetyypit, joilla sisältöä saa käyttää,
- sekä mediaoperaatiot, jotka esimerkiksi määrittelevät saako sisältöä siirtää CD:lle tai laitteelta toiselle.

DRM nähdään usein arvokkaan sisällön suojelemisena jakelijayhtiön toimesta. Yhtä hyvin digitaalisen sisällön suojelemisen ongelmaa voidaan katsoa yleisesti tarpeena valvoa johdonmukaisia tietoihinpääsykontrolleja, jotka perustuvat yhden tai useamman asianosaisen määrittelemiin käytöntöihin [CoM06]. Asianosainen voi olla kuluttaja, joka antaa yksityisyyden suojan alaista tietoa itsestään, tai sairaalan rekisteri, jolla on sekä laillinen että eettinen velvollisuus suojella potilaiden sairaskertomuksia.

Nykyisten DRM-tekniikoiden tavanomaisimpia ongelmia ovat niiden rajoittuminen tukemaan vain tietynlaisia sisältömuotoja ja tekniikoita, sekä se, etteivät ne salli oikeuksien siirtämistä [ZYX07] laitteelta toiselle, eivätkä käyttäjältä toiselle. Tämä on aiheuttanut kiivastakin DRM:n vastustamista esimerkiksi musiikin kuuntelijoiden keskuudessa. Toisaalta joillekin ajatus sisällön ”vuokraamisesta” sen ostamisen sijaan tuntuu liian vieraalta.

2.3 Yhteistyöverkostojen tarpeet sisällön suojaamiselle

Tämän tutkielman puitteissa DRM-tekniikoita käsitellään pääasiassa yhteistyöverkostoissa tapahtuvan sisällön jakamisen kannalta. Yhteistyöverkostoissa halutaan jakaa tarvittava tieto kaikille osallistujille, mutta pitää kuitenkin huolta siitä, että tiedon omistajuus säilyy alkuperäisellä taholla, eikä tieto vuoda luvatta yhteisön ulkopuolelle. Jos tietoa huomataan vuotaneen, halutaan tietää vastaisuuden varalle, kuka on pettänyt yhteisön luottamuksen

tietoa eteenpäin jakamalla. Digitaalisen sisällön helppo käytön hallinta, ja toisaalta digitaalisen sisällön yksilöllinen merkitseminen niin, ettei merkintää saa ainakaan helposti poistettua, ovat esimerkkejä hyvän DRM-järjestelmän kriteereistä yhteistyöverkostoihin.

Organisaatiot kääntyvät enenevässä määrin erilaisten yhteistyöverkostojen puoleen pysyäkseen kilpailukykyisinä [BVD08]. Sekä sosiaalisten että liiketoimintaan liittyvien yhteistyöverkostojen lisääntyessä on herätty huomaamaan sensitiivisen tiedon liikkumisen lisääntyminen. Nykyiset sovellukset eivät kuitenkaan tarjoa riittävää yksityisyydensuojaa näissä yhteistyöverkostoissa toimijoille [SMM11]. Kun tuottaja jakaa tietoja tuotteestaan tai prosesseistaan, se samalla asettaa immateriaalioikeuksiaan alttiiksi riskille levitä myös asiattomiin käsiin. Kauppiaan myyntiennusteiden ilmitulo kilpailijoille voi viedä kauppiaan altavastaajan asemaan.

Organisaatiot voivat jossain käyttää salassapitosopimuksia näiden riskien välttämiseksi [BVD08]. Ne voivat kuitenkin olla työläitä neuvotella ja valvoa, joten tehokkaampia vaihtoehtoja tarvitaan. Tähän tarpeeseen vastaavat tietokonesovellusten käyttäjäkontrollit. Olemassa olevat käyttökontrollit ovat kuitenkin yleensä ohjelmistopohjaisia, joten niiden kiertämiseen löytyy ohjeita ja tekniikoita, jopa julkisilta Internetsivuilta. Lisäksi niihin ei ole olemassa standardia, joten eri laitteistovalmistajien tuotteet eivät yleensä toimi keskenään. Lisäksi käytön kontrolloinnista yhteistyöverkostoissa tiedetään vielä liian vähän. Jos käytön kontrollointi keskeyttää yhteistyön työnkulun, se pudottaa helposti yhteistyöstä odotetut edut miinuksen puolelle.

Sisällön käytön kontrollointi voi lisätä turvallisuutta yhteistyöverkostoissa. Brustolonin et al [BVD08] tutkimuksessa käytön kontrolloinnilla oli vain merkityksettömän pieni vaikutus käytön helppouteen (mitattuna käytetyn ajan ja tehtävien suorittamisen tarkkuuden perusteella). Käyttäjät osasivat hyväksyä sopivat politiikat omalle käytölleen vain minimaalisen opastuksen jälkeen, suorituskyvyn heikkenemättä. Käytön kontrollointi on siis yksi hyvä ehdokas digitaalisen sisällön oikeuksien hallintaan yhteistyöverkostoissa.

Kaupallisessa kontekstissa yksityisyyden suoja määrittelee sen, millä tavalla organisaatiot ja yksilöt voivat kontrolloida tietojen keräämistä, käyttöä ja jakamista, henkilökohtaiset, suojeltavat tiedot mukaan lukien [PeM11].

Yksityisyyden suojan takaaminen, ja sekä lakien että yleisesti käytössä olevien ohjeiden noudattaminen lisää asiakkaiden luottamusta organisaatioon. Yksityisyyden suojaan Internet-aikakaudella on kohdistettu paljonkin tutkimusta. Tutkimuksen kohteena ovat usein anonymiteettiteknologiat ja toisaalta erilaisten yhteisten säädöksien ja toimintatapojen kehittäminen esimerkiksi EU:n alueella. Avoimia kysymyksiä on kuitenkin vielä paljon: miten saada loppukäyttäjälle suurempi kontrolli, miten kerätä ja hallinnoida loppukäyttäjien antamia suostumuksia, ja miten pitää yllä tehokasta yksityisyyden suojan hallintaa tiedon siirtyessä ryhmältä toiselle.

Yksi lähestymistapa on liitetyt politiikat (sticky policies) – tietoon liitetyt ehdot ja rajoitteet, joilla määritellään miten sisältöä tulisi kohdella. Data saattaa olla salakirjoitettua, ja siihen pääsee käsiksi vain vaadittujen menettelytapojen täytyttyä [PeM11]. Erityisesti nämä menettelytavat kuvaavat tiedon käyttötapoja, ja niiden avulla voidaan määritellä seuraavia asioita:

- tiedon käytön syy – tutkimusta, transaktion toteuttamista tms. varten
- tiedon käyttö vain sellaisilla alustoilla, joilla pystytään takaamaan toivotuntasoinen tietoturva, esim. jossain aliverkossa
- velvoitteet tai kiellot, kuten saako näyttää kolmansille osapuolille prosesseille
- mustat listat, ilmoitus tiedon paljastumisesta, tietojen vähentäminen tai kokonaan poistaminen tietyn ajan jälkeen
- tiedot luotetuista tahoista, joiden kautta tietoon on mahdollista saada käyttöoikeuksia jonkinlaisen neuvotteluprosessin tuloksena.

Liitetyt politiikat tarjoavat lupaavan vaihtoehdon yksityisyyden hallintaan sekä organisaation rajojen sisällä että organisaatioiden välillä, vaikka pilvipalveluiden kautta. Luotettujen osapuolten kautta tapahtuva tiedonkulun jäljitys ja auditointi auttaa vahvistamaan, että käyttäjän asettamia ehtoja noudatetaan.

3 Erilaisia DRM-tekniikoita

DRM-menetelmiä on useita erilaisia. Oikeastaan kyse onkin toisiinsa lomittuvista tekniikoista, joiden avulla voidaan luoda turvallinen jakelukanava

digitaaliselle sisällölle. DRM:n avulla voidaan rajata tunnistettu käyttäjäjoukko, joilla on oikeus päästä käsiksi tietoon jonkin median avulla. Karkeasti jaettuna menetelmät jakaantuvat itse sisällön merkitsemiseen ja suojaamiseen, käytön valvontaan, sekä petturin jäljittämiseen (traitor tracing) perustuviin tekniikoihin. Näitä erilaisia DRM-tekniikoita ovat tiedon salakirjoittaminen, tiedon muuttamisen estäminen, kopioinnin määrien tai tapojen kontrollointi, tekijänoikeusmerkinnät, digitaaliset vesileimat ja sormenjäljet sekä muut autentikointimenetelmät.

3.1 DRM:n funktiot sisällön eri elinkaarivaiheissa

Sisällön elinkaaren eri vaiheissa myös sisällönhallinnan oikeuksien suojaamisen funktiot ovat erilaisia. Sisältöä luotaessa korostuu sisällön suojaaminen, sisältöä jaettaessa ja käytettäessä sen käytön valvonta, ja sisällön elinkaaren loppupäässä petturien jäljittäminen eli laittoman käytön selvittäminen.

3.1.1 Sisällön suojaaminen

Sisällön salakirjoittaminen (encryption) on yksinkertainen DRM-tekniikka. Tieto salakirjoitetaan jonkin salausalgoritmin ja avaimen avulla. Avain, jonka avulla salakirjoituksen voi purkaa, annetaan sisällön laillisille käyttäjille [SuB06]. Digitaalisia allekirjoituksia käytetään sekä sisällön tarjoajien että sisällön käyttäjien tunnistamiseen.

Symmetrisessä salauksessa kaikilla käyttäjillä/laitteilla, jotka aikovat jakaa salattua tietoa, tulisi olla salausavain hallussaan jo etukäteen. Asymmetrisessä salauksessa jokaisella kommunikoinnin osapuolella on julkinen ja salainen avain. Tietylle käyttäjälle suunnattu tieto salataan tämän julkisella avaimella, jonka hän taas pystyy omalla salaisella avaimellaan avaamaan.

Sekä sisällön salakirjoittaminen että käyttäjien autentikointi ovat tekniikoita, jotka estävät digitaaliseen sisältöön pääsyn laittomilta käyttäjiltä. Autentikoinnissa voidaan käyttää digitaalisten allekirjoitusten lisäksi erilaisia salasanoja, todistuksia jne. Jos pahantahtoinen käyttäjä onnistuu kuitenkin kiertämään nämä tekniikat, hän saa sisällön haltuunsa täysin suojaamattomana ja alttiina laittomille muokkauksille [TsP08].

3.1.2 Käytön valvonta

Käytön kontrollointi antaa sisällön jakelijalle mahdollisuuden määrittää, miten sen vastaanottajat saavat käyttää ko. tiedostoa, esim. onko tiedoston tulostaminen sallittu [BVD08]. Käyttöoikeudet määrittelevät tarkasti, miten sisältöä voidaan käyttää. Erilaisia loppukäyttäjälle sallittuja tai kiellettyjä **käyttöoikeuksia** voidaan määritellä esimerkiksi päivämäärän tai ajanjakson, käyttökertojen, alusta- ja laitetyyppien ja mediaoperaatioiden kautta.

Käytön hallinta voidaan asettaa sisältöön automaattisesti, nopeasti ja edullisesti, joten ne ovat houkutteleva vaihtoehto tai lisä sisällön suojaamiseen. Käyttäjät eivät koe käyttörajoitteisten sisältöjen käyttöä erityisen hankalana, eikä sopivien käyttötapojen valinta tuota heille ongelmia [BVD08]. Useimmat käytönhallintamekanismit ovat kuitenkin sovelluspohjaisia ja helppoja purkaa. Niitä voi vahvistaa laitteistopohjaisilla käyttökontrolleilla.

Käytön valvonta on erityisesti kaupallisella puolella (musiikkiteollisuus) eniten vastustusta herättänyt mekanismi. Ostaja haluaa tehdä hankkimallaan sisällöllä mitä haluaa, ei käyttää ostostaan vain viisi kertaa tietyssä yksittäisessä laitteessa. Vahvan kopiointisuojan rinnalle onkin siellä noussut muita strategioita, joilla kuluttajaa houkutellaan ostamaan digitaalista sisältöä laillisten kanavien kautta [RBP09].

Käytön hallintaan on kehitetty myös omia alakohtaisia kieliä [LJB11], joilla voidaan ilmaista sallitut käyttötavat ja määrittää mitkä menettelytavat liittyvät mihinkin tuotteeseen. Käytön hallintaa voidaan määritellä niiden avulla yksityiskohtaisemmin kuin pelkän tiedon suojaamisen tai siihen pääsyn kautta, selkeästi ja yksiselitteisesti.

Jokaisella käyttöoikeudella oma syntaksi ja semantiikka, jotka määritellään käyttöoikeuskielellä. Sisältöön liittyy tietty muoto (DRM content format). Sisältö ja siihen liittyvät oikeudet yhdistetään DRM-viestiksi, jonka perusteella sisällön toistava laite tietää miten sisältö kuuluu esittää. DRM-viestin puuttuessa käytetään oletusarvoja [SuB06].

3.1.3 Petturin jäljittäminen

Petturin jäljittämisessä oletetaan, että salakirjoituksen purkulaitteet ovat ”avoimia” niin, että lailliset käyttäjät tietävät oman purkulaitteensa yksityisen purkuavaimen [JoL11], ja että jokaisella purkulaitteella on oma yksityinen avain, jonka avulla purkulaite (ja sen omistaja) voidaan identifioida. Ideaalisti purkulaiteet olisivat mahdottomia kajota, jolloin laite ja sen sisältämät avaimet olisivat suojassa laittomalta käytöltä. Silloin niitä ei myöskään voisi kloonata, joten salausavain voisi olla sama kaikissa. Älykortit ovat tällaisia peukalointia vastustavia, kloonamattomia ratkaisuja.

Sisällön jäljittämisessä myyjä lisää sisältöön jonkin uniikin merkkijonon (eli sormenjäljen), joka edustaa ostajan identiteettiä [PoZ11]. Näin merkitty kopio annetaan ostajalle alkuperäisen sisällön sijasta. Jos merkitystä kopiosta tehtyjä uusia kopioita löytyy myöhemmin laittomasta jakelusta, voi myyjä selvittää syyllisen sormenjälkeä tutkimalla. Ongelmaksi jää, että myyjällä on täysi kontrolli sekä sisällön, sormenjäljen että sen jäljityksen suhteen: jos laiton kopio löytyy, myyjä ei voi todistaa sitä laittomaksi; ostaja voi väittää tulleensa lavastetuksi, ja luoda epäluuloa jäljitysjärjestelmää kohtaan.

BSW-prokolla (buyer-seller watermarking protocol, ostajan-myyjän vesileimausprotokolla) ja asymmetrinen sormenjälkitekniikka esiteltiin vastaamaan näihin ongelmiin. Molemmat toteutetaan myyjän ja ostajan yhteistyönä. Luotettu kolmas osapuoli yhdistää sisältöön ostajan vesileiman. Silti turvallisuusriskejä löytyy oston uusinnan (jossa pahantahtoinen osapuoli on nauhoittanut käydyt keskustelut, ja lähettää ne uudestaan luotetulle osapuolelle, joka laskuttaa uudelleen alkuperäistä asiakasta) ja muunteluhyökkäyksien muodossa, tai ainoan luotetun osapuolen saadessa liikaa luottamusta osakseen.

Korkealuokkainen sisältö on yleensä salakirjoitettua, jotta sen jakelua saadaan kontrolloitua. Luvallisille käyttäjille annetaan laitteisto- tai ohjelmistopurkaja, joka sisältää salakirjoituksen purkuun tarvittavan avaimen. Tällaisia salauksenpurkulaitteita saatetaan yrittää rakentaa laittomasti itse. **Petturin jäljittäminen** (traitor tracing) tarkoittaa, että selvitetään ainakin jonkun sellaisen

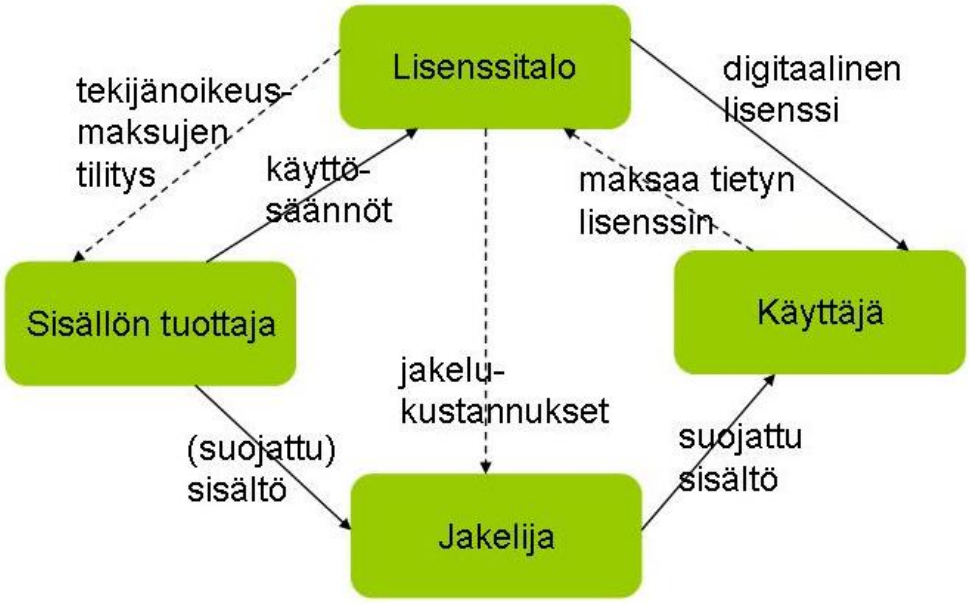
laillisen käyttäjän henkilöllisyys, joka on ollut mukana rakentamassa laitonta sisällön salauksen purkulaitetta [JoL11].

3.2 Erilaisia DRM-mekanismeja

Sisällön elinkaaren eri vaiheiden erilaisiin vaatimuksiin sopivat erilaiset DRM-mekanismit. Seuraavaksi esitellään niistä tärkeimpiä.

3.2.1 DRM-lisenssijärjestelmä

Tyypillinen DRM-järjestelmä koostuu kuluttajien käyttämistä esityslaitteistoista, jotka kommunikoivat sisältöpalvelimen ja lisenssipalvelimen kanssa verkon kautta [Sub06]. Verkko voi olla lähes minkätyyppinen verkko tahansa, sisäverkosta Internetiin tai langattomaan yhteyteen. Sisältöpalvelimella on tarjolla haluttu sisältö johonkin sopivaan tiedostomuotoon pakattuna. Lisenssipalvelin luo ja hallinnoi lisenssejä, jotka sisältävät tiedon siitä, mitä oikeuksia voi hankkia mille sisällölle ja minkälaiselle käyttäjälle tai laitteelle. Tästä esimerkki näkyy kuvassa 1. Käyttäjän esityslaitteiston pitää tukea valittua DRM järjestelmää ja pystyä tulkitsemaan oikein lisenssiin määriteltyjä sääntöjä ja oikeuksia.



Kuva 1 Esimerkki DRM-lisenssijärjestelmästä.

Sisällön ja sen käyttöoikeudet ovat siis erillisiä. Itse sisältöä voidaan jakaa ja ladata vapaasti; sitä ei kuitenkaan voi käyttää ilman voimassa olevaa lisenssiä, johon on määritelty asianmukaiset oikeudet.

Sisältöä voidaan hankkia joko jollekin kannettavalle mediavälineelle tallennettuna (CD, DVD, mp3) tai verkon välityksellä joko kerralla tallennettuna (download), jolloin sitä käytettäessä sisältöön yhdistetään tarvittava lisenssi, tai suoratoistona (streaming), jolloin sitä ei tallenneta käyttäjän millekään laitteelle, ja sisältövirta suojataan ennen jakelua sen omilla salakirjoitusmekanismeilla, jotka vastaanottava laite osaa purkaa ja toistaa sisällön oikein. Tällaiset salattuna lähetykset ovat tulleet yhä tärkeämmäksi kaupallisissa tarkoituksissa, esimerkiksi maksu-TV:n myötä, jossa lähetyskeskuksesta lähetetetään palvelu suurelle käyttäjäjoukolle turvatonta kanavaa pitkin, omistajan oikeuksia suojellen.

Eri salakirjoitustekniikoissa itse sisältö voi olla joko vapaasti jaettavissa, mutta käytettävissä vain lisenssin kanssa, tai itse sisältökin voi olla suojattu salakirjoituksella, jonka avaavan avaimen lailliset käyttäjät voivat hankkia. Sekä sisällön tuottajien että sisällön käyttäjän tunnistaminen tapahtuu yleensä digitaalisen allekirjoituksen avulla. Allekirjoitus todennetaan joko lisenssiä myönnettäessä, tai kun käyttäjän laite ottaa yhteyden lisenssipalvelimelle soittaakseen hallinnoimaansa sisältöä tai uusiakseen lisenssin tarvittaessa. Lisenssipalvelimen osoite on tallennettuna sisällön otsikkoon muiden metatietojen mukana.

Itse lisenssi sisältää käyttöoikeudet [SuB06], eli ehdot ja olosuhteet jotka liittyvät sisällön käyttöön. Lisenssiin kuuluu myös avain, jolla sisällön saa avattua, jos se on salakirjoitettu. Lisenssi voidaan hankkia lisenssipalvelimelta tai toimittaa sisällön mukana, jopa käyttäjän edes tietämättä lisenssin mukana olosta. Lisenssi voi vain sallia sisällön käytön, tai se voi purkautua jos lisenssiä käytetään väärin, jolloin sisältöä ei voi enää käyttää.

DRM-sovelluksen kehittämisessä on erityisen kriittistä huolehtia mahdollisimman vähäisestä tiedon vuotamisesta järjestelmän ja sen kehittäjien

ulkopuolelle [KIN05]. Kaikki turvallisuustiedot salausavaimista alkaen on säilytettävä oikein salassapidettyinä.

Joskus yksityisyyden suojalla on käyttäjälle suurempi merkitys kuin sisällöstä maksettavalla maksulla [PKP10]. Tähän ratkaisuksi on ehdotettu esimerkiksi anonyymin rahan käyttöä, jossa käyttäjä on saanut pankilta salattuna käyttöönsä pankin allekirjoittaman maksusitoumuksen tietylle summalle, tai sokeaa salakirjoitusta, joka toimii yhdessä monien eri salakirjoitusten, kuten esimerkiksi RSA:n kanssa. Sokeassa salakirjoituksessa ideana on, että salakirjoitettu keskustelu ei salaa käyttäjän identiteettiä, vaan se on sisällön tuottajan tiedossa, mutta sisällön tuottaja ei tiedä minkä tuotteen käyttäjä sisältövalikoimasta hankki itselleen. Tämä on paljon tehokkaampi ja edullisempi tapa tehdä yksityisyyden suojan ylläpitäviä ostoksia kuin anonyymin rahan käyttö, koska anonymisointi-infrastruktuuria ei tarvita [PKP10]. Anonyymin rahan käyttö mahdollistaa tekijänoikeusmaksut, sokeassa salakirjoituksessa sisällön ostokertoja ei ole mahdollista laskea. Molemmat tavat tukevat lisävaltuutustekniikoita, joilla sisällön käyttöä voidaan hallita salausavainten avulla, ja molemmissa tavoissa käyttäjän on vain luotettava siihen, että kaupanteko toteutuu sovittujen sääntöjen mukaan, eikä yksityisyyden suojalle ole uhkaa.

3.2.2 Digitaalinen vesileimaus

Digitaalinen vesileimaus (digital watermarking) nojaa itse sisällön merkitsemiseen. Se on siis yksi sisällönsuojaustavoista, joilla tehdään tekijänoikeusmerkintöjä suoraan suojeltavaan sisältöön. Digitaalista vesileimausta käytetään useimmiten kun tekijänoikeuksia on suojeltava, ja sisältö on sellaisten ryhmien saatavilla, joilla saattaa olla syitä vesileimauksen poistoon [TsP08]. Käytännössä digitaalisessa vesileimauksessa upotetaan sisältöön tekijänoikeuslauseita; tieto sisällön luojasta, tuottajasta, ja käytön ehdoista [SuB06]. Vesileimaus on yleensä huomaamaton, ja aina huomiota herättämätön [CYY98]. Yritys poistaa digitaalinen vesileima huonontaa heti tuotteen laatua. Useat vesileimaustavat heikkenevät hyökkäysten lisääntyessä tai niiden aiheuttaessa epäsynkronointia itse tuotteeseen. Niinpä tärkein vaihe digitaalisessa vesileimauksessa onkin sopivan vesileimausalgoritmin valinta

[TsP08]. Useimmissa vesileimausalgoritmeissa salaista avainta käytetään määrittämään upotusfunktion ominaisuuksia kuten upotusalue, upotuksen suunta, tai kuvan kertoimien osajoukko, joka vesileimataan [PCT06]. Vesileimauksen näkymättömyyttä on lisätty esimerkiksi vesileimausalgoritmin moduloinnilla pseudosatunnaisen, tai Gaussin sarjan avulla. Kuvien merkinnässä käytettään myös ns. tilkkutäkkiä, jolloin kuvan pseudosatunnaisesti valituista kahdesta pikselijoukosta toisia kirkastetaan ja toisia himmennetään. Erilainen ratkaisu on käyttää salaista avainta vesileimauksen löytämisen funktion valintaan salaisesta taulukosta. Näissä kaikissa ratkaisuissa vesileima ja digitaalinen sisältö ovat itsenäisiä, erillisiä osia. Reunainformoiduissa (side-informed) tekniikoissa perusidea on vastakkainen: sisältö itsessään vaikuttaa vesileiman laskentaan. Tästä esimerkkinä voidaan mainita QIM-metodit (quantitazation index modulation), joissa salaista avainta käytetään generoimaan salainen koodikirja isäntäkuvan kvantittamiseen, ja vesileima on käytännössä kvanttivirhe isännän ja salaisen kvantittimen välillä, ja Millerin et al metodi. Siinä vesileima luodaan siten, että ensin jokainen viesti kuvautetaan sarjaksi säleikön polkuja, ja jokainen säleikön muunnos assosioituu joukkoon avain-riippuvaisia leviäviä vektoreita. Tällöin purkaminen tehdään etsimällä se säleikön polku, joka maksimoi korkeimman korrelaation vastaanotetun signaalin ja kaikkien siihen polkuun liittyvien leviävien sekvenssien välillä [PCT06].

Digitaalisen vesileimauksen yhteydessä on keskusteltu ennen kaikkea vesileimauksen vankkuudesta (robustness, mikä voidaan määritellä salauksen purun virheen todennäköisyydellä tai vesileiman poistamisen vastustuskyvyllä [PCT06]), sekä sen huomaamattomuudesta ja kapasiteetista, ja lähes unohdettu vesileimauksen turvallisuuskysymykset. Koska monet vesileimojen turvallisuuteen liittyvät ongelmat ovat samoja kuin tietoturvaan ja salakirjoituksiin liittyvät kysymykset, kannattaa niiden tutkimisessa kerätty tietämys hyödyntää vesileimaustekniikoita kehitettäessä [LMS06]. Vesileimauksessa tulisi käyttää tunnettuja avaimenvaihtoprotokollia, tiedonsalausta ja lähteen autentikointia, ja lisätä luotettavuutta jakamalla tietoa ja varmistuksia useamman eri auktoriteetin eli luotetun osapuolen kesken [PoZ11]. Vesileimauksen turvallisuus on suoraan verrannollinen salausavaimen

arvioinnin helppouteen tai vaikeuteen, kaiken hyökkääjän tekemän havainnoinnin pohjalta [PCT06].

Joskus vesileimauksen tarkoituksena on vain lisätä sisällön arvoa, tai linkittää sisältö Internetiin tai tietokantaan, tämäntyyppiset vesileimaukset harvoin joutuvat hyökkäyksen kohteeksi [PCT06]. Sen sijaan lääketieteellisten kuvien, laillisten dokumenttien autentikaation tai tiedon monitoroinnin täytyy varautua hyvinkin vihamielisiin ympäristöihin. Aina ei ole kysymys edes vesileiman poistoyrityksistä, vaan lakiin liittyvissä kysymyksissä on joskus haitallisempaa hyväksyä väärennetty sisältö kuin olla hyväksymättä aito.

Tekijänoikeuksien suojaamiseksi kannattaa sisältöön lisätä kaksi vesileimaa: ensimmäinen käyttää tekijänoikeuden omistajan salaista avainta hänen omistusoikeutensa julistamiseen, ja toinen vesileima jotain julkista vakioavainta, joka julistaa sisällön olevan kopiointikiellossa [TsP08]. Tällaisen tunnistavien laitteiden käyttöönotto kaikkialla vaatisi sitä tukevaa lakia.

Omistusoikeuden määrittäviä sovelluksia vastaan on olemassa erityyppisiä hyökkäyksiä, joiden avulla voidaan määritellä digitaalisen vesileimauksen turvallisuuden vähimmäisvaatimuksia. Digitaalisen vesileimauksen tavoitteenahan on vakiinnuttaa digitaalisen sisällön oikeat omistusoikeudet tekemällä alkuperäisestä sisällöstä suojattu versio, jonka variantitkin voidaan jäljittää sisällön alkuperäiseen omistajaan. Näin ajateltuna omistajuuden suojelevalla järjestelmällä on kolme osaa: vesileiman luominen, istuttaminen ja havaitseminen. Varkaalla on tällöin muutama mahdollinen tapa hyökätä suojausta vastaan: hankkia alkuperäistä vastaavat todisteet, että on sisällön alkuperäinen omistaja, jolloin omistajuutta ei voida päätellä ja syntyy lukkiuma, hankkia alkuperäistä paremmat todisteet siitä, että on sisällön alkuperäinen omistaja (väärennetty omistajuus), tai suojata laiton kopionsa omalla suojauksellaan ja sen kautta väittää koko sisältöä omakseen (omistajuuden varastaminen). Vesileimaukseen perustuva järjestelmä voidaan luokitella turvalliseksi, jos mikään edellä mainituista ei onnistu. Sen edellytyksenä on:

- vankkuus (robustness)
- matala väärien positiivisten todennäköisyys
- upotuksen purkamattomuus

- luotetun osapuolen mukanaolo.

Koska kaikkein triviaalein hyökkäys digitaalisella vesileimalla suojattua sisältöä vastaan on vesileiman poistoyritys, on ensimmäisenä turvallisuusvaatimuksena vesileimaustekniikan vankkuus kaikkea mahdollista pahantahtoista muokkaamista vastaan.

Kohdista viimeistä, luotetun osapuolen mukanaoloa, voidaan pitää jopa ehtona sille, että vesileimauksesta voidaan puhua turvallisena [AKV03]. Nykytutkimuksen mukaan turvallisuus riippuu suurelta osin pohjana olevan vesileiman huomaamismekanismista, eikä kaikkialla käyttökelpoista, universaalia konstruktiota pystytäkään tekemään.

Digitaalista vesileimausta voidaan käyttää myös jonkin sisällön personointiin tietylle käyttäjälle ja käyttäjäryhmälle.

3.2.3 Digitaaliset sormenjäljet

Digitaaliset sormenjäljet (digital fingerptints) ovat digitaalisten vesileimojen tapaan tiedonpalasia upotettuna itse sisältöön. Piilotettuja merkintöjä on käytetty jo vuosisatoja tekijänoikeuksia rikkovan, laittoman jakelun jäljittämiseen [LMS06]. Toisin kuin vesileimoissa, digitaalisissa sormenjäljissä jokainen kopio saa oman uniikin koodin, joka helpottaa sen omistajan identifiointia, ja toisaalta niiden jäljittämistä, jotka ovat laittaneet oman kopionsa laittomasti jakoon.

Digitaalisia sormenjälkiä käytetään usein juuri petturin jäljittämiseen, tai toisaalta sisällön autenttisuuden ja oikeellisuuden toteamiseen.

Sovelluspohjaisissa lähestymistavoissa on joitakin etuja. Ne ovat halvempia ja helpompia jakaa ja päivittää, ja niiden peukalointi (tampering) pystytään estämään monimutkaistamalla tekniikoita tarkoituksenmukaisesti, ja salaustekniikoita ja hash-funktioita käyttämällä.

3.2.4 Laitteistopohjaiset salaustekniikat

Laitteistojen salaustekniikoita ovat esim. CD-levyjen lohkoihin sisällytetyt rakennetiedot, jotka kopioitaessa tulkitaan tyhjiksi ja täten hypätään koko sektorin yli [Vas09]. Myös CD-levyjen alikanavia voidaan käyttää lisäinformaation säilyttämiseen, kuten alkuperäisten ja kopioiden toisistaan

erottamiseen. Kaksoissektoreita käyttämällä voidaan myös erottaa alkuperäiset levyt kopioiduista.

Toinen teknologia, jolla luvattomat käyttäjät suljetaan sisällön ulkopuolelle, on donglet. Dongle on pieni laitteisto esim. USB-muistitikussa, jonka yksilöllinen sarjanumero täytyy olla kytkettynä kohteeseen salatun sisällön paljastamiseksi. Donglet eivät ole kovin laajasti levinneitä, lähinnä niiden sisällölle tuottaman lisähinnan vuoksi.

Myös **luotettu tietojenkäsittely** voidaan laskea laitteistojen salaustekniikaksi. Alusta tai tila, jossa DRM-suojattu tieto suoritetaan, katsotaan vihamieliseksi, joten käyttäjän on taattava turvallinen ympäristö, jossa tieto pysyy suojeltuna, saadakseen sen käyttöönsä. Luotettu tietojenkäsittely tarjoaa seuraavat piirteet: turvallisen tietojen siirron käyttäjän ja ohjelmiston välillä, piilossa olevat salausavaimet ja muu turvallisuusinformaatio, ja sinetöidyn varastoinnin, mikä tarkoittaa että digitaaliseen tietoon päästään käsiksi vain oikein laitteiston ja ohjelmiston välityksellä, eikä ilman sille kuuluvaa lisenssiä. Itse luotettuun ympäristöön käyttäjällä ei ole mitään oikeuksia.

Luotettu tietojenkäsittely onkin saanut osakseen kritiikkiä siitä, että se antaa suurten yritysten määrätä miten ohjelmistoalustoja käytetään, eikä käyttäjä voi vaikuttaa omaan interaktioonsa tiedon kanssa [CoM06]. Turvallisissa ratkaisuissa näin onkin välttämättä meneteltävä, on kontrolloitava miten tietoon pääsee käsiksi. Tämä ei kuitenkaan tarkoita, että kuluttajalta pitäisi viedä kontrolli pois kokonaan, vaan hänen tulee voida valita vapaasti käyttämänsä käyttöjärjestelmät ja sovellukset, mikä onkin mahdollista.

4 DRM-tekniikoiden sopivuus yhteistyöverkostoihin

Digitaalisen tiedon jakaminen yhteistyöverkostoissa vaatii joitakin ominaisuuksia digitaalisilta oikeuksienhallintamenetelmiltä. Digitaalinen tieto halutaan antaa verkoston jäsenten käyttöön yhteistyön edistämiseksi, mutta sisältö itsessään halutaan suojata, ja pitää selkeänä se, kuka tietosisällön omistaa, sekä estää laiton edelleen jakelu.

Liitetyt politiikat tarjoavat lupaavan lähestymistavan yksityisyydenhallintaan organisaation rajojen sisällä ja yli, ja niitä voidaan käyttää monissa muissakin

sovelluksissa, kuten pilvipalveluissa [PeM11]. Sisällön omistaja määrittelee sallitut käyttötavat (liitetyt politiikat) julkaistessaan tiedot organisaatiolle. Ne määrittelevät sallitut käyttötavat ja takaavat että sopivia rajoitteita käytetään, jollakin takuulla. Liitettyjen politiikkojen käyttö antaa mahdollisuuden tiedon seurantaan ja auditointiin luotettujen auktoriteettien kautta, ja sisällön omistajan asetusten toimeenpanon palveluntarjoajan kautta.

muista lisätä [TsP08] ratkaisu

5 Yhteenveto

Digitaalisen sisällön oikeuksien hallintaa ei tarvitse nähdä vain mediayhtiöiden tekijänoikeuksien alaisen jakelun kontrollointina. Yhtä lailla DRM tarjoaa yrityksille ja yhteisöille mahdollisuuden suojella niiden arkaluonteisen tiedollisen omaisuuden käyttöä, tai käyttäjille yksityisyyden suojaa verkossa.

Sisällön eri elinkaarivaiheissa erilaisten DRM-tekniikoiden käyttökelpoisuus vaihtelee. Yhteistyöverkostoissa…

Lähteet

AKV03 Adelsbach, A., Katzenbeisser, S., Veith, H., Watermarking Schemes Provably Secure Against Copy and Ambiguity Attacks. Proceedings of the 3rd ACM workshop on Digital rights management, New York, NY, USA, 2003, sivut 111-119.

Boy11 Boyden, B. E., Is DRM Working? How Could We Tell? Proceedings of the 11th annual ACM workshop on Digital rights management, New York, NY, USA, 2011, sivut 1-2.

BVD08 Brustoloni, J. C., Villamarin-Salomon, R., Djalaliev, P., Kyle, D., Evaluating the Usability of Usage Controls on Electronic Collaboration. Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08), Pittsburgh, PA, USA, 2008, sivut 85-92.

CoM06 Cooper, A., Martin, A., Towards an open, trusted digital rights management platform. Proceedings of the 8th ACM workshop on Digital rights management, Alexandria, VA, USA, 2006, sivut 79-87.

CYY98 Craver, S., Yeo, B.-L., Yeung, M., Technical Trials and Legal Tribulations. Communications of the ACM, Vol. 41, 7 (1998), sivut 45-54.

Die08 Diehl, E., A four-layer model for security of digital rights management. Proceedings of the 8th ACM workshop on Digital rights management, Alexandria, VA, USA, 2008, sivut 19-27.

DoK08 Doërr, G., Kalker, T., Design Rules for Interoperable Domains: Controlling Content Dilution and Content Sharing. Proceedings of the 8th ACM workshop on Digital rights management, Alexandria, VA, USA, 2008, sivut 39-49.

ElA07 Elkamchouchi, H., Abouelseoud, Y., Digital Rights Management System Design and Implementation Issues. Proceedings of ICCES'07, International Conference on Computer Engineering & Systems, Cairo, Egypt, 2007, sivut 120-125.

ETD03 Eskicioglu, A. M., Town, J., Delp, E. J., Security of Digital Entertainment Content from Creation to Consumption. Signal Processing: Image Communication, Vol 18, 4 (2003), sivut 237–262.

JoL11 Joye, M., Lepoint, T., Traitor Tracing Schemes for Protected Software Implementations. Proceedings of the 11th annual ACM workshop on Digital rights management, New York, NY, USA, 2011, sivut 15-21.

JSS11 Jafari, M., Safavi-Naini, R., Sheppard, N. P., A Rights Management Approach to Protection of Privacy in a Cloud of Electronic Health Records. Proceedings of the 11th annual ACM workshop on Digital rights management, Chicago, Illinois, USA, 2011, sivut 23-29.

KIN05 Kanzaki, Y., Igaki, H., Nakamura, M., Monden, A., Matsumoto, K., Characterizing Dynamics if Information Leakage in Security-Sensitive Software Process. Proceedings of the 2005 Australasian workshop on Grid computing and e-research, Darlinghurst, Australia, 44 (2005), sivut 145-151.

LJB11 Lamb, C. C., Jamkhedkar, P. A., Bohnsack, M. P., Nandina, V., Heileman, G. L., A Domain Specific Language for Usage Management. Proceedings of the 11th annual ACM workshop on Digital rights management, Chicago, Illinois, USA, 2011, sivut 51-62.

LMS06 Li, Q., Memon, N., Sencar, H. T., Security Issues in Watermarking Applications – A Deeper Look. Proceedings of the 4th ACM international workshop on Contents protection and security, Santa Barbara, California, USA, 2006, sivut 23-27.

OwA04 Owens, R., Akalu, R., Legal Policy and Digital Rights Management. Proceedings of the IEEE, 92, 6 (2004), sivut 997-1003.

PCT06 Perez-Freire, L., Comesana, P., Troncoso-Pastoriza, J. R., Perez-Gonzalez, F., Watermarking Security: A Survey. Transactions on Data Hiding and Multimedia Security, LNCS 4300, 2006, sivut 41-72.

PeM11 Pearson, S., Mont, M. C., Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer, 11 (2011), sivut 60-68.

PKP10 Perlman, R., Kaufman, C., Perlner, R., Privacy-Preserving DRM. Proceedings of the 9th Symposium on Identity and Trust on the Internet, New York, NY, USA, 2010, sivut 69-83.

PoZ11 Poh, G. S., Z'aba M. R., On the Security and Practicality of Buyer Seller Watermarking Protocol for DRM. Proceedings of the 4th international conference on Security of information and networks, New York, NY, USA, 2011, sivut 251-254.

RBP09 Regner, T., Barria, J. A., Pitt J.V., Neville, B., An artist life cycle model for digital media content: Strategies for the Light Web and the Dark Web. Electronic Commerce Research and Applications 8 (2009), sivut 334-342.

SMM11 Shen, Y., Miettinen, M., Moen, P., Kutvonen, L. Privacy Preservation Approach in Service Ecosystems. Proceedings of 15th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW), Helsinki, Finland, 2011, sivut 283-292.

SRZ06 Sandhu, R., Ranganathan, K., Zhang, X., Secure Information Sharing Enabled by Trusted Computing and PEI Models. Proceedings of the 2006 ACM Symposium on Information, computer and communications security, New York, NY, USA, 2006, sivut 2-12.

SuB06 Subramanya, S. R., Byung, K. Y., Digital rights management. IEEE Potentials, 25, 2 (2006), sivut 31-34.

TsP08 Tsolis, D. K., Papatheodorou, T. S., Web services for digital rights management and copyright protection in digital media. Proceedings of the 3rd international conference on Digital Interactive Media in Entertainment and Arts, Athens, Greece, 2008, sivut 241-247.

ZYX07 Zhaofeng, M., Yixian, Y., Xinxin, N., Secure and Flexible Digital Rights Management in a Pervasive Usage Mode. Proceedings of International Conference on Computational Intelligence and Security, Harbin, China, 2007, sivut 863-867.