Oskari Oksanen

Digitaaliset rajoitukset tietokonepelien suojauksessa

Tietotekniikan kandidaatintutkielma

27. huhtikuuta 2015

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Oskari Oksanen

Yhteystiedot: osaneeok@student.jyu.fi

Työn nimi: Digitaaliset rajoitukset tietokonepelien suojauksessa

Title in English: Digital restrictions in computer game protection

Työ: Kandidaatintutkielma

Sivumäärä: 21+0

Tiivistelmä: Digitaalinen käyttöoikeuksien hallinta — lyhennettynä DRM — on ollut yksi peliteollisuuden kiistellyimmistä keinoista hillitä piratismia Internetin kaupallistumisen jälkeen. Vaikka menetelmää pidettiin alunperin välttämättömyytenä pelialalle, pelaajat ja jopa pelinkehittäjät ovat väittäneet menetelmän olevan vain haitaksi laillisille pelaajille ja pikemminkin houkuttelevan käyttäjiä piratoimaan pelinsä sen seurauksena. Tässä tutkielmassa käsitellään aluksi digitaalista käyttöoikeuksien hallintaa yleisesti, Internetin yleistymistä edeltäneitä tietokonepelien suojausmenetelmiä ja lopuksi neljää DRM-pohjaista suojausmenetelmää tietokonepelialalta.

Avainsanat: drm, digital rights management, tietokonepelit, piratismi, kopiosuojaus

Abstract: Digital rights management — DRM for short — has been one of gaming industry's most controversial methods to combat piracy since the commercialization of the Internet. While DRM was initially deemed as a necessity for the industry, gamers and even game developers have claimed that the method only serves as a hindrance for legal customers and that it tempts people to pirate their games because of that. This thesis first examines digital rights management in general, computer game protection methods used before the widespread usage of the Internet, and lastly four DRM methods used in the computer games.

Keywords: drm, digital rights management, computer games, piracy, copy protection

Sisältö

1 Johdanto

Internet on nykyään melkein kaikkialla, se on kiistaton fakta. Yksi sen huomattavimmista piirteistä on pitkään ollut tiedon nopea jakaminen käyttäjältä toiselle, sekä hyvässä että pahassa. Nettipiratismi on ollut yksi yleisimmistä kitkemisyrityksien kohteista, ja yksi näistä kitkemistavoista on digitaalinen käyttöoikeuksien hallinta, lyhennettynä DRM. Kyseinen termi kattaa kaikki digitaaliset menetelmät, joilla on tarkoitus estää digitaalisen tuotteen tai palvelun laitonta käyttöä ilman vaadittavia tunnistetietoja.

DRM:n tarkoitus ollessa hyvä, useat tahot pelialalla ovat kuitenkin jättäneet konseptin väittäen sen aiheuttavan vain turhaa työtä sekä pelinkehittäjille että pelaajille (ks. Holm 2014, s. 66–69). Tutkielmassani aion tarkastella, mitkä ovat syyt suojaustavan suosion laskulle pelialalla, vaikka piratismi on edelleen vahvasti läsnä.

Luvussa 2 käsitellään yleisesti digitaalisen käyttöoikeuksien hallinnan syitä ja seurauksia, sekä DRM-menetelmien yleisimpiä toimintatapoja. Luvussa 3 käsitellään tietokonepelien suojausmenetelmiä, jotka olivat yleisessä käytössä ennen Internetin yleistymistä. Luvussa 4 käsitellään neljää tietokonepelien DRM-suojausmenetelmää, joita pelinkehittäjät ovat Internetin yleistymisen jälkeen käyttäneet peliensä turvaksi.

2 Digitaalinen käyttöoikeuksien hallinta

Digitaalinen käyttöoikeuksien hallinta (engl. *Digital Rights Management*) viittaa kaikkiin digitaalisiin toimintamenetelmiin, joiden tarkoituksena on rajoittaa tuotteiden laitonta käyttöä julkaisun jälkeen, yleensä ohjelmallisin keinoin. Vaikka määritelmään sopivia menetelmiä on ollut olemassa jo 1970-luvulla, muun muassa levykkeiden suojauksessa (Layton 2006, s. 2; Basinger 2012, 2:41–3:15), DRM käsitteenä syntyi kuitenkin vasta 1990-luvun loppupuolella alan tavarantoimittajien ja analyytikoiden keskuudessa (Rosenblatt, Mooney ja Trippe 2001, s. vii).

Yhdeksi huomattavimmaksi syyksi DRM:n synnylle pidetään Internetin kaupallistumista, sekä kehittymistä uutena jakelukanavana 1990-luvun aikana (Rosenblatt, Mooney ja Trippe 2001, s. x–xi). Yleistymisen myötä tuottajilla oli helpompaa jakaa digitaalisia tuotteitaan eteenpäin, mutta aikaisimmat yritykset suojata niitä pohjautuivat käsitykseen, että digitaaliset tuotteet olisivat kauppatavaroina olleet yhtä helposti käsiteltävissä ja myytävissä kuin fyysiset tuotteet. Varhaisimpia DRM-menetelmiä kehitettiinkin suurimmalta osin tämän näkemyksen pohjalta, minkä seurauksena tuottajat keskittyivät kehittämään ainoastaan tuotteidensa kopiosuojausta. Tätä suuntautumista pidetäänkin yhtenä syynä sille, miksi varhaisimmat käytänteet eivät loppujen lopuksi toimineetkaan odotetulla tavalla; kun piraatit saivat kuorittua sisällön ulos kopiosuojauksestaan, materiaalin laittomalle levittämiselle ei olisi ollut mitään muuta käytännön estettä. (Rosenblatt, Mooney ja Trippe 2001, s. 19) DRM-menetelmiin viitaaminen ylimalkaisesti termillä kopiosuojaus on todennäköisesti jäänyt elämään juuri näiltä varhaisilta ajoilta.

Kopiosuojauksen ollessa edelleen tärkeä osa DRM:ää, nykymuodossaan menetelmät kattavat monia muitakin suojauskäytänteitä, joita käsitellään tarkemmin luvussa 2.2. Varhaisimmat menetelmät eroavat toimintaperiaatteiltaan viimeisimmistä kuitenkin sen verran, että nämä kokeelliset menetelmät on tapana erottaa vakiintuneemmista suojauskäytänteistä kahdeksi erilliseksi sukupolveksi.

2.1 Sukupolvet

Ensimmäisen sukupolven menetelmät keskittyivät suojauskeinoissaan pääosin rajoittamaan vain kopioimista. Käyttäjät pystyivät kyllä halutessaan jakamaan suojattua ohjelmaa eteenpäin melko vapaasti, mutta käyttäjän olisi tarvinnut antaa uudet tunnistetiedot joka kerta, kun hän olisi halunnut käyttää ohjelmaa uudessa koneessa. (Gaber 2013, s. 71) Yksinkertaisimpana esimerkkinä pelialalta voidaan pitää vanhoja tietokonepelejä, jotka asennuksen yhteydessä vaativat pelin mukana tulostettua aktivointikoodia pelin avaamiseksi (ks. 3.4).

Toisen sukupolven — tai toisin sanoen nykyiset — menetelmät taas pyrkivät laajimmillaan rajoittamaan ja valvomaan tuotteen käyttöä kokonaisuudessaan. Kyseisten menetelmien kautta kehittäjillä on mahdollisuus määrätä, kuinka heidän tuotteitansa voi muokata, tarkastella, tai ylipäätänsä käsitellä julkaisun jälkeen. (Layton 2006, s. 3) Pelialalla yksi tunnetuimmista esimerkeistä on Steam-palvelu, mikä pelilisenssien myymisen ja käyttäjäkohtaisten pelikirjastojen ylläpitämisen lisäksi mahdollistaa käyttäjiään pelaamaan pelejään millä tahansa tietokoneella pelkkien käyttäjätunnuksien kautta (ks. 4.4).

Tutkielman aihealueen rajoittamiseksi, tulen tästä eteenpäin DRM-menetelmistä yleisesti puhuessani viittaamaan vain toiseen sukupolveen.

2.2 Toimintatavat

Erilaisuuksistaan huolimatta Van Tassel (2006, s. 77–117) väittää DRM-menetelmien olevan yleistavoitteiltaan luokiteltavissa — joko kokonaisuudessaan tai osittain — neljään seuraavaan kategoriaan:

- sisällön suojaus,
- sisällön saatavuuden rajoitus,
- sisällön kopioinnin rajoitus ja
- sisällön välityksen rajoitus.

Sisällön suojaus viittaa menetelmiin, joiden toimintaperiaatteet perustuvat suojattavan sisällön dynaamiseen muokkaamiseen, muiden käytänteiden suojatessa tiedostoja pitkälti vain ulkopuolisesti. Konkreettisimpana esimerkkinä tästä voidaan pitää tiedostojen salausta (engl.

encryption), mikä on yleistä muun muuassa tiedostonsiirtojen yhteydessä. Tällöin tiedoston rakenne sekoitetaan systemaattisesti tietyn suojausavaimen (engl. *encryption key*) mukaisesti, siirretään tiedosto salattuna toiseen sijaintiin, ja palautetaan tiedosto tavalliseksi toisella suojausavaimella. Suojausavaimet voivat olla joko julkisia tai yksityisiä (engl. *public key* ja *private key*). Sisällön suojaus saattaa ilmentyä myös pelkkänä sormenjäljen kaltaisen tunnisteen lisäämisenä, jolloin menetelmää käytetään yleensä osana suurempaa suojauskokonaisuutta.

Saatavuuden rajoitus kattaa oikeuksien hallintaan pohjautuvia suojausmenetelmiä, joiden kautta määritellään, kuinka käyttäjä tai jokin muu taho pystyy käsittelemään sisältöä. Toimintatapa on käytännössä tuttu kaikille tietokoneen käyttäjille salasanojen ja nettitunnuksien kautta. Yleisimmissä tapauksissa käyttäjä antaa palvelulle tai ohjelmistolle pyydettäessä tietyt tunnistetiedot, ja näiden tietojen pohjalta käyttäjälle annetaan näihin tietoihin liittyvät sisällön käsittelyoikeudet, esimerkiksi oikeudet käydä läpi tiliin liitettyjä sähköpostiviestejä. Tunnistetiedot saattavat olla myös sidoksissa laitteistoon tai ohjelmistoon. Tällaisissa tilanteissa tunnistukset ja oikeuksien hallinnat voidaan suorittaa ilman minkäänlaista vuorovaikutusta käyttäjän kanssa. Tästä voidaan pitää esimerkkinä DVD-laitteiden ja -levyjen aluekoodausta (engl. *region code*).

Kopioinnin rajoitus käsittää sisällön dataan sidottuja suojausmenetelmiä, pyrkien dataan upotettujen tunnisteiden kautta hillitsemään kopiointia. Toimintatavan aikaisimmat edustajat pyrkivät pääosin rajoittamaan aikansa uuden tallennusvälineen, DVD-levyn sisällön kopioimista. Yksi näistä menetelmistä estikin toistolaitteita jakamasta dataa eteenpäin muihin kytköksissä oleviin laitteisiin, jos toistava laite olisi tunnistanut jakamisen eston vaativia tunnistetietoja. Tietokonekäyttäjien keskuudessa tämän kategorian edustajana voidaan pitää salattujen PDF-tiedostojen tapaa estää tekstin suora kopioiminen ja liittäminen (engl. *copy-and-paste*). Menetelmän yksi suurimmista ongelmista on kuitenkin edelleen ihmisten kyky kopioida sisältöä analogisin keinoin, kuten nauhoittamalla TV-ruutua videokameralla tai kopioimalla salattua tekstiä manuaalisesti. Tähän eston kiertämistapaan viitataan yleensä termillä analoginen reikä (engl. *analog hole*).

Välityksen rajoitus on laitteistoihin ja ohjelmistoihin sidottu suojausmenetelmä, suunniteltu suojaamaan digitaalista sisältöä siirtovaiheessa. Ennen datan lähettämistä, lähde- ja tois-

tolaitteen pitää tunnistaa toisensa molemminpuoleisesti, ja jos jokin ei täsmää, lähdelaite voi estää lähettämisen kokonaan. Yksi toimintatavan käytännemalleista perustuu myös sisällön suojauksesta tuttuun tiedoston salaamiseen: lähdelaite sekoittaa sisällön, lähettää sekoitetun sisällön kohti päämääräänsä, ja saapuessaan vastaanottolaite muuttaa sisällön takaisin ymmärrettävään muotoon. Tätä kautta lähteen ja vastaanottajan väliset laitteet eivät pääse käsiksi siirrettävään sisältöön.

Yksittäisiä DRM-menetelmiä tarkastellessa on kuitenkin tärkeä huomioida, että tuottajat soveltavat yleensä useampaa kuin yhtä yllä listattua toimintamallia sisältönsä suojaamiseksi. Jotkut saattavat salata tiedostonsa (sisällön suojaus), lähettää tiedoston käyttäjälle, mutta käyttäjä saa käsiinsä tiedoston salauksen avaavan avaimen vasta, kun hän on antanut avaimen luovutukseen oikeuttavat tunnistetiedot (saatavuuden rajoitus).

3 Vanhat suojausmenetelmät

Osa pelinkehittäjistä olivat jo ennen DRM:n käsitteen keksimistä pyrkineet hillitsemään tietokonepeliensä piratointia erilaisilla kopiosuojausmenetelmillä, joista osa oli jo käytössä 1970-luvulla. Nämä menetelmät saattoivat olla vain tietokonepeleille ominaisia suojausratkaisuja, kun taas osassa sovellettiin muissa digitaalisissa tuotteissa käytettyjä kopiosuojauskeinoja. Osaa näistä menetelmistä voidaan myös pitää osana DRM:n ensimmäistä sukupolvea, kuten aiemmin kuvailtu luvussa 2.1. Hyams (2008, s. 11–23) ja Basinger (2012, 2:41–10:39) käsittelevät joitain tunnetuimpia DRM:n toista sukupolvea edeltäneiltä suojausmenetelmiä, jotka voidaan toimintatavoiltaan jakaa seuraavanlaisiin kategorioihin:

- levysidonnainen kopiosuojaus,
- avainsanasidonnainen kopiosuojaus,
- fyysiset lukot,
- aktivointikoodit ja
- hämäystiedot.

3.1 Levysidonnainen kopiosuojaus

Levysidonnainen kopiosuojaus on menetelmä, jolla suojatut pelit hyödyntävät pelin fyysisen tallennusvälineen ominaisuuksia varmistaakseen kopion aitouden, ja oli yksi yleisimmistä tavoista suojata levykkeitä (engl. *floppy disk*). Pelinkehittäjät saattoivat peliä fyysiseen muotoon tallennettaessa muokata osan levykkeestä tahallisesti käyttökelvottomaksi, mitä ohjelmakoodissa sitten käytettiin virallisten kopioiden tunnistamiseksi ja näin ollen pelin avaamiseksi. Tämän ominaisuuden takia suojattuja levykkeitä kutsuttiin usein myös nimellä avainlevy (engl. *key disk*), koska ohjelmaa ei voitu avata ilman levykkeen todentamista. Koodin sitominen tietyn tyyppisesti muunneltuun levykkeeseen esti siis tätä kautta ohjelman suoran kopioimisen tavanomaisille levykkeille tai kovalevylle.

Kovalevyjen yleistyessä suojattujen pelien levykesitoisuus kuitenkin muodostui vähitellen yleiseksi ärtymyksen aiheeksi pelaajien keskuudessa. Levykkeiden hauraan olemuksen vuoksi käyttäjät toivoivat pystyvänsä tekemään peleistä omia varmuuskopioita ja mahdollisesti

jopa pelaamaan niitä kovalevyltä, mutta suojatut levykkeet eivät tätä mahdollisuutta sallineet. Tietokoneiden kehittyessä pelinkehittäjät alkoivatkin vähitellen etsimään uudenlaisia suojauskeinoja vastaamaan pelaajien tarpeisiin.

3.2 Avainsanasidonnainen kopiosuojaus

Avainsanasidonnainen kopiosuojaus on menetelmä, jolla suojatut pelit eivät varsinaisesti estä piratoiduilla kopioilla pelaamista, mutta vaativat pelien mukana saatujen oheistuotteiden käyttöä läpipääsemiseksi. Yksinkertaisimmissa tapauksissa peli saattoi pyytää käyttäjää kirjoittamaan tietyn sanan pelin ohjekirjan tietyltä sivulta, minkä peli tulkitsisi laillisen kopion merkiksi ja antaisi käyttäjän jatkaa pelaamista normaalisti. Osa pelinkehittäjistä menivät asiassa kuitenkin tätäkin pidemmälle ja jakoivat pelien mukana juuri vastaavia tarkastuksia varten laadittuja koodikiekkoja ja -listoja (engl. *code wheel* ja *code sheet*). Kiekot ja listat saattoivat olemukseltaan vaihdella suurestikin pelistä riippuen, mutta yksi yleisimmistä tavoitteista oli tehdä koodien kopioiminen — ja sitä kautta levittäminen — mahdollisimman työlääksi aikansa piraateille.

Ongelmaksi menetelmälle muodostui kuitenkin riippuvaisuus pelin ulkopuoliseen materiaaliin. Vaikka pelaajalla olisi ollut laillinen kopio pelistä, tarkastukseen tarvittavien oheistuotteiden hukkaaminen olisi estänyt koko pelin pelaamisen. Myöhemmässä vaiheessa myös kopiokoneiden kehittyminen sai pelinkehittäjät vähitellen keksimään muunlaisia suojauskeinoja.

3.3 Fyysiset lukot

Fyysisten lukkojen käyttö on toinen oheistuotepohjainen suojaustapa, mutta koodilistojen sijaan pelien mukana jaettiin enemminkin mekaanisia lisätarvikkeita auttamaan pelien todennuksessa. Koottuihin salasanakokoelmiin verrattuna kyseiset lukot olivat paljon vaikeampia jäljentää perinteisin keinoin. Oheistuote saattoi esimerkiksi olla vain todennusta varten luotu tietokoneadapteri, joka piti liittää tietokoneeseen tietyllä tavalla ennen kuin ohjelman sai tietokoneelta auki.

Pelialalla yksi tunnetuimmista — muttei tosin pidetyimmistä — fyysisistä lukoista oli optiikkaan pohjautuva lisätarvike nimeltään *Lenslok*. Ennen pelin avaamista, tietokone esitti ruudulla kaksi vääristettyä kirjainta, mitkä käyttäjä sai näkymään ainoastaan katsomalla pelille tarkoitetun Lenslok-linssin läpi tietystä kulmasta ja tietyn kokoiselta näytöltä. Jälkimmäinen seikka osoittautui pelaajille turhauttavimmaksi, sillä linssi ei toiminut liian isojen tai pienien näyttöjen kanssa, minkä seurauksena osa laillisistakaan pelaajista eivät päässeet pelaamaan lukon taakse suojattuja pelejään. Ja kuten koodilistojen kanssa, pelille tarkoitetun linssin tai muunkaan lukon hukkaaminen olisi estänyt pelin pelaamisen kokonaan.

3.4 Aktivointikoodit

Osa varhaisista CD-pohjaisista peleistä eivät sisältäneet minkäänlaista kopiosuojausta, osittain aikansa kovalevyjen normitallenuskapasiteetin vuoksi. Tavallinen CD-levy saattoi sisältää enemmän dataa kuin tavalliselle kovalevylle olisi mahtunut, mikä jo itsessään toimi varsin tehokkaana kopiosuojauskeinona. Kovalevyjen kehittyessä ja tallennuskapasiteetin kasvaessa pelinkehittäjät alkoivat kuitenkin vähitellen kehittämään kopiosuojauksia myös CD-peleille.

Aktivointikoodit (engl. *serial keys*) olivat yksi yleisimmistä tavoista todentaa CD-pelien aitoutta asennuksen jälkeen. Ennen kuin peliä pystyi pelaamaan ensimmäistä kertaa, käyttäjän piti pyydettäessä syöttää pelin mukana saatu koodisarja, joka toimi tunnisteena pelin avaamiseksi. Tämän jälkeen peliä pystyi pelaamaan koneelta vapaasti, myös ilman pelin CD-levyä.

Menetelmän ollessa pelaajille varsin helppokäyttöinen se oli yhtä lailla myös yksi heikoimmista kopiosuojausmenetelmistä, koska aktivointikoodit eivät välttämättä olleet sidottuna yksittäisiin tietokoneisiin. Tällaisissa tilanteissa pelin mukana saatua koodia olisi pystynyt käyttämään täysin vapaasti, eli helposti jakamaan sellaisenaan eteenpäin. Internetin yleistyminen auttoi kuitenkin myöhemmässä vaiheessa sitomaan koodit yksittäisiin tietokoneisiin ja mahdollisesti myös rajoittamaan asennuskertoja pääosin Internetin kautta tehtävien todennusten avulla, mikä on edelleenkin yleinen kopiosuojausmenetelmä.

3.5 Hämäystiedot

Hämäystietojen käyttö viittaa menetelmiin, jotka pohjautuvat virheellisten tietojen tahalliseen sisällyttämiseen CD-levyille. Nämä virheelliset tiedot saattavat ilmetä niin, että tietokoneen pyytäessä levy antoi tahallisesti liioitellun arvion tallennuskapasiteetistaan, tai levylle sisällytettiin tarkoituksella ylisuuria täytetiedostoja viemään tilaa. Näitä keinoja kehittäjät pyrkivät käyttämään enemminkin pelotteena aikansa piraateille, koska kopioidessaan tiedostot eivät olisi välttämättä mahtuneet tietokoneen kovalevylle, eikä pelille olennaisimpia tiedostoja pystytty erottamaan tyhjästä täytteestä.

Ajan myötä kovalevyjen ja kopiointiohjelmien kehitys teki kyseisen menetelmän kuitenkin hyödyttömäksi laitonta kopioimista vastaan. Myös Internetin saatavuuden ja nopeuden kasvaessa, piraateilla ei ollut enää mitään käytännön estettä jakaa suojauksesta riisuttuja pelejä eteenpäin. Tässä vaiheessa pelinkehittäjät alkoivatkin soveltamaan suojauskeinoissaan DRM-suojausmenetelmiä.

4 Käyttöoikeuksien hallinta tietokonepeleissä

Pelien kopiosuojausyritykset ovat pohjautuneet suurimmalta osin aikansa tietoteknisiin rajoitteisiin pelinkehittäjien pyrkiessä mukailemaan menetelmiään tekniikan kehityksen mukana, kuten luvusta 3 voi nähdä. Kun Internetin kehitys oli vähitellen päätynyt pisteeseen, että pelit olivat paljon helpommin saatavilla ilmaiseksi netistä kuin maksullisesti kaupasta, oli vain ajan kysymys, milloin pelinkehittäjät alkaisivat soveltamaan Internet-pohjaisia keinoja suojaamaan pelejään. Pelinkehittäjät ovatkin tätä kautta päätyneet erilaisten DRM-pohjaisten suojausmenetelmien käyttöön vuosien varrella, mistä tulen käsittelemään seuraavaa neljää:

- SecuROM,
- StarForce,
- FADE ja
- Steam.

4.1 SecuROM

SecuROM on Sony DADC -yrityksen kehittämä suojausohjelmisto, joka on suunniteltu suojaamaan sekä levyjä että tiedostoja. Ohjelmiston levysuojaus perustuu virallisen levyn tunnistukseen, joka suoritetaan levyyn upotetun allekirjoituksen (engl. *signature*) kautta. Jos tarkistusta vaativa ohjelma ei saa tunnistettua levyä tätä kautta viralliseksi, käyttäjä saa virheilmoituksen, eikä kone käynnistä ohjelmaa. SecuROM-ohjelmiston tiedostojen suojaus toimii pitkälti samalla periaatteella, paitsi vaadittava digitaalinen tunniste asennetaan käyttäjän tietokoneelle ohjelman asennuksen yhteydessä Internetin kautta. (*General information about SecuROM*)

Tietokonepeleissä SecuROM nähdään kuitenkin enemmänkin ärsykkeenä kuin hyötynä pelaajien keskuudessa toimintatapojensa vuoksi. Yleisimmät seikat, joita tuodaan esille suojausohjelmistoa haukkuessa on pelien asennuskertojen rajoitettu määrä, suojattujen levyjen yhteensopimattomuus tiettyjen levyasemien kanssa, sekä SecuROM-ohjelmiston tunnisteiden epäilyttävä luonne. Pelien vaatimia tunnistetiedostoja on tiedettävästi asennettu ilman

käyttäjien tietämystä, minkä lisäksi tiedostot eivät ole välttämättä poistuneet järjestelmästä pelin asennusta poistettaessa. Osa pelaajista onkin tästä syystä epäillyt tunnistetiedostojen väitettyjä tarkoitusperiä, jotkut jopa väittäen niitä osaksi vakoiluohjelmaa (engl. *spyware*), mutta kyseisten tiedostojen tarkkailevista tarkoitusperistä ei ole löytynyt mitään konkreettista näyttöä. (Ghazi 2012, s. 9; Anderson ja Renzulli 2009, s. 27–28) Tästä huolimatta pelijulkaisijat ovat aika ajoin ottaneet SecuROM-suojauksia pois käytöstä jälkikäteen, yleensä pelaajien painostuksesta (ks. Caron 2008).

4.2 StarForce

StarForce on sarja StarForce Technologies -yrityksen kehittämiä suojausohjelmistoja, jotka keskittyvät pelien suojaamisen lisäksi muun muassa sähköpostien ja dokumenttitiedostojen suojaukseen. Pelien suojaukseen yrityksellä on nykyään tarjolla kolme erillistä suojausohjelmistoa: vain tiedostoja suojaava, vain pelilevyjä suojaava ja molempia suojaava. (*StarForce Products*) Tiedostojen suojauksessa peli varmistaa käyttäjän oikeudet aktivointikoodin ja käyttäjän koneesta kerättyjen tietojen pohjalta (*StarForce ProActive*), kun taas levyjen suojaus pohjautuu ajoitettuun levyn tarkistukseen (*StarForce Disc*).

StarForce tunnettiin aikanaan yhtenä vaikeimmin purettavista DRM-suojauksista. Yhdessä tunnetuimmassa tapauksessa suojauksen purkaminen kesti yli vuoden (ks. Ciolek 2009). SecuROM-ohjelmiston tapaan StarForce on tiedettävästi asentanut pelien tunnistamiseen vaadittuja tiedostoja ilman käyttäjien suostumusta, aiheuttaen samantapaisia — sekä yhtä lailla perättömiä — vakoiluepäilyjä, minkä lisäksi StarForce-ohjelmiston väitettiin aiheuttavan toiminnoillaan käyttöjärjestelmien kaatumista, hidastumista ja jopa levyasemien vahingoittumista. Näitä väitteitä sekä ohjelmiston kehittäjien reaktiota kritiikille (ks. Anderson 2006a; EDGE 2008, s. 4) pidetään huomattavimpina syinä sille, että StarForce on pelaajien keskuudessa edelleen yksi inhotuimmista DRM-suojausmenetelmistä, vaikka ohjelmiston vahingollisesta käytöksestä ei olekaan löytynyt mitään konkreettista näyttöä. (Ghazi 2012, s. 9) Osa pelijulkaisijoista onkin lopettanut StarForce-ohjelmiston käytön peleissä SecuROM-ohjelmiston lailla pelaajien painostuksesta (ks. Anderson 2006b).

4.3 FADE

FADE — tunnetaan myös nimellä DEGRADE (Grayson 2011, s. 1) — on CodeMasters-yrityksen kehittämä suojausmenetelmä, jonka käytänteet perustuvat digitaalisten naarmujen tunnistamiseen. Suojauksen idea perustuu siihen, että kopiointiohjelmat korjaisivat tahallisesti sisälletyt naarmut pelin dataa kopioidessa, ja tätä kautta peli ei pystyisi todentamaan kopiota aidoksi. FADE ei kuitenkaan estä laittomilla kopioilla pelaamista, mutta sellaisen tunnistaessaan peli alkaa hiljalleen heikentämään toimintojaan, kunnes käyttäjä ei pysty enää jatkamaan pelaamista. (Fox 2003; CodeMasters 2001) SecuROM- ja StarForce-ohjelmistoista poiketen kyseinen suojausmenetelmä ei asenna erillisiä tunnistetiedostoja pelin asennuksen yhteydessä.

Pelialalla FADE tunnetaan parhaiten Bohemia Interactive -kehittäjän ARMA-pelisarjasta, jossa suojausmenetelmää on käytetty sarjan alusta lähtien. Armeijatoimintaan pohjautuvana pelisarjana FADE vaikuttaa sen mukaisiin ydintoimintoihin: pelaaja saattaa kokea aseiden tarkkuuden heikkenemistä, ajoneuvojen satunnaista jarruttelua ja kaasuttelua, sekä äärimmäisissä tapauksissa aseettomaksi linnuksi muuttumista. (Grayson 2011, s. 1; Gerardi, Teti ja Toal 2013) FADE-menetelmää on kehuttukin valistavasta lähestymistavastaan pelien suojaukseen (ks. Plunkett 2011), mutta tästä huolimatta menetelmää — tai pelitoimintojen muokkausta ylipäätänsä — ei ole käytetty vakituisena suojausperiaatteena missään muussa pelisarjassa.

4.4 Steam

Steam on Valve Corporation -yrityksen luoma digitaalisten tietokonepelien jakelualusta, mikä hoitaa pelien suojauksia Internet-pohjaisten tunnistusten kautta. Käyttäjä pystyy luomaan palveluun ilmaisen käyttäjätilin, jota kautta käyttäjä pystyy ostamaan pelien lisenssejä ja niiden kautta lataamaan pelejä tietokoneelleen. Useammalla käyttäjällä on mahdollisuus kirjautua samalle koneelle ja käyttää samoja pelitiedostoja, mutta Steam sallii jokaisen käyttäjän pelata vain niitä pelejä, joihin heillä on voimassa olevat lisenssit. Tätä kautta käyttäjä ei pääse pelaamaan muiden Steam-pelejä, vaikka hänellä olisikin pelin vaatimat tiedostot. (*What is Steam*)

Steam-alustaa pidetään nykyään malliesimerkkinä digitaalisesta pelien jakelupalvelusta, mutta tämä ei kuitenkaan tarkoita, että se olisi sellaisena täydellinen. Yksi yleisimmistä valituksen aiheista ovat käyttäjien kykenemättömyys jälleenmyydä pelejään eteenpäin sekä tilanteet, että Valve-yrityksen todennuspalvelimien kaatuessa käyttäjät eivät pystyisi todentamaan ja sitä kautta pelaamaan pelejään. Lisäksi on puhuttu tilanteesta, että palvelun lopettaessa toimintansa käyttäjät saattaisivat menettää oikeutensa ostamiinsa peleihin ilman minkäänlaista korvausta. Palvelusta olisikin jo tätä kautta yhtä paljon aihetta valittaa kuin SecuROM- tai StarForce-ohjelmistosta, mutta kritiikin vähäisyyden uskotaan yksinkertaisesti johtuvan Valve-yrityksen suosiosta pelialalla sekä Steam-alustan että pelien kehittäjänä. (Ghazi 2012, s. 9; Basinger 2012, 12:57–13:34)

5 Yhteenveto

Digitaalisella käyttöoikeuksien hallinnalla on pyritty antamaan digitaalisten tuotteiden kehittäjille välineitä hillitsemään laitonta levittämistä ja tätä kautta turvaamaan tuottajien tuloja. Menetelmien käyttö on kuitenkin saanut osakseen lähinnä vieroksuntaa ja inhoa sekä pelaajien että pelinkehittäjien keskuudessa, osa jopa väittäen menetelmien houkuttelevan käyttäjiä hankkimaan pelinsä laittomasti välttäkseen suojausehtojen kanssa painimisen. Vaikka väite ei pitäisikään paikkansa, on kuitenkin selvää että DRM-pohjaiset menetelmät voivat häiritä laillisilla kopioilla pelaavia, pahimmillaan vaikuttaen jopa suoraan pelikokemukseen. (ks. Holm 2014, s. 66–69)

SecuROM- ja StarForce-ohjelmistot käyttävät suojauksessaan ohjelmasta erillisiä tiedostoja, jotka asennetaan pelien asennuksen yhteydessä, mutta nämä tiedostot eivät välttämättä poistu pelejä poistettaessa. Tämä on ollut yksi huomattavimmista seikoista, minkä takia osa pelaajista on leimannut nämä kaksi ohjelmistoa vakoilu- ja haittaohjelmiksi (engl. *spyware* ja *malware*), vaikka kummankaan vahingollisesta luonteesta ei olekaan vedenpitävää näyttöä. (Ghazi 2012, s. 9) Tästä voidaan ajatella, että pelaajat eivät ole pystyneet epäilyksiensä kanssa luottamaan tarpeeksi näiden suojausohjelmistojen väitettyihin toimintatapoihin kehittäjien selityksistä huolimatta (ks. *The truth about StarForce drivers; General information about SecuROM*). Tämä luottamuspula on sitten johtanut äänekkääseen vastustukseen ja huhujen levittämiseen, mitä kautta pelaajat alkoivat menettämään luottamusta myös suojauksia käyttäviä pelijulkaisijoita kohtaan, joissakin tapauksissa johtaen lopulta suojausten käytöstä poistamiseen (ks. Caron 2008; Anderson 2006b).

FADE-menetelmä perustuu koodiin sisällettyjen virheiden tunnistamiseen, jonka pohjalta peli joko toimii normaalisti tai heikentää hiljalleen pelinaikaisia toimintoja (Fox 2003; CodeMasters 2001). Vaikka menetelmää onkin kehuttu tavastaan soveltaa DRM:ää (ks. Plunkett 2011), FADE on toiminut vakituisena suojausmenetelmänä vain Bohemia Interactiven ARMA-pelisarjassa (Grayson 2011, s. 1). Yleistyessään pelitoimintojen muuntaminen voisi kuitenkin suojaumenetelmänä vastata yhteen yleisimmistä syistä, millä pelaajat perustelevat pelien piratoimista: pelien lataaminen kokeilumielessä. Koska FADE ei estä laittomilla kopiolla pelaamista, pelaaja voisi saada pelin käsiinsä jo ensimmäisenä myyntipäivänä, ja pe-

lata sitä niin kauan, kunnes peli alkaa muuttamaan toimintojaan. Tällaisissa tilanteissa olisi kuitenkin tärkeää, että pelaajalle annettaisiin tarpeeksi aikaa tutustua peliin ennen toimintojen muuttamista sekä tähdentää pelaajalle, minkä takia peli alkaa käyttäytymään oudosti.

Steam-palvelu ylläpitää käyttäjätileihin sidottuja pelikirjastoja ja käsittelee näiden kautta pelien käyttöoikeuksia, sallien käyttäjien pelata palvelusta ostettuja pelejä miltä tahansa tietokoneelta (*What is Steam*). Helppokäyttöisyydestään huolimatta palvelu ei salli pelien jälleenmyymistä tai niiden käynnistämistä ilman palvelun käynnistämistä, mistä ei ole kuitenkaan valitettu yhtä äänekkäästi kuin muista rajoittavista DRM-menetelmistä. Tämän uskotaan johtuvan Valve-yrityksen suosiosta pelialalla, minkä voidaan katsoa kertovan pelaajien luottamuksesta yritystä kohtaan. (Ghazi 2012, s. 9; Basinger 2012, 12:57–13:34) Tästä huolimatta palvelun riippuvuus yhteen yritykseen on seikka, mikä olisi hyvä ottaa huomioon kaikkien digitaalisten pelien jakelupalveluiden tulevaisuuden kannalta. Nykytilanteessa Valve-yrityksen lopettaminen päättäisi samalla Steam-palvelun pelien jakelun, pelikirjastojen ylläpidon ja pahimmillaan käyttäjien oikeudet ostamiinsa peleihin.

Kaikissa DRM-menetelmissä on yleisenä ongelmana se, että mikään niistä ei ole tarkoitettu kestämään ikuisesti. Vaikka suojaukset olisivatkin läpipääsemättömiä tavallisille käyttäjille, pelin suojauksen purkamiseksi ei välttämättä tarvita kuin yksi kykenevä käyttäjä, joka voi purkamisen jälkeen laittaa pelin kaikille vapaasti jaettavaksi Internetiin. Tämä onkin yksi seikoista, mihin osa pelaajista vetoaa perustellessaan DRM-menetelmien tehottomuutta: kun piraatit saavat kuorittua sisällön ulos DRM-suojauksestaan, materiaalin laittomalle levittämiselle ei olisi mitään muuta käytännön estettä. Tätä kautta voidaankin ajatella, että DRM kamppailee edelleen saman ongelman kanssa kuin syntyessään, eikä piratismi näytä yrityksistä huolimatta minkäänlaisia laantumisen merkkejä. Osa pelinkehittäjistä ovatkin luultavasti ottaneet tästä opiksi ja päättäneet keskittyä enemmän pelinkehitykseen, mutta niin kauan kuin käyttäjät piratoivat pelejä, on oletettavissa että kehittäjät pyrkivät suojaamaan niitä tavalla tai toisella.

Lähteet

Anderson, B., ja E. Renzulli. 2009. *Modern Digital Rights Management Methods.* Kandidaatintutkielma. Saatavilla verkosta: <http://www.wpi.edu/Pubs/E-project/Available/E-project-051109-135624/>. Viitattu 31.1.2015. Worcester Polytechnic Institute, Massachusetts, USA.

Anderson, N. 2006a. "Is your games copy protection system frying your machine?" Saatavilla verkosta: <http://arstechnica.com/uncategorized/2006/01/6084-2/>. Viitattu 14.4.2015. *Ars Technica.*

———. 2006b. "Its official: Ubisoft dumps StarForce". Saatavilla verkosta: <http://arstechnica.com/uncategorized/2006/04/6603-2/>. Viitattu 14.4.2015. *Ars Technica.*

Basinger, C. 2012. *LGR - History of DRM & Copy Protection in Computer Games.* Video, pituus 17:09. Saatavilla verkosta: <http://www.youtube.com/watch?v=HjEbpMgiL7U>. Viitattu 26.2.2015.

Caron, F. 2008. "EA games officially come to Steam, sans DRM". Saatavilla verkosta: <http://arstechnica.com/gaming/2008/12/ea-games-officially-come-to-steam-sans-drm/>. Viitattu 5.4.2015. *Ars Technica.*

Ciolek, T. 2009. "Interview: The Return Of... StarForce?" Saatavilla verkosta: <http://www.gamasutra.com/php-bin/news_index.php?story=24035>. Viitattu 14.4.2015. *Gamasutra.*

CodeMasters. 2001. "Codemasters continues to fight a cold war against game piracy in preparation for the release of Operation Flashpoint in early September". Saatavilla verkosta: <http://web.archive.org/web/20080207222153/http://www.codemasters.com/press/?showarticle=500>. Viitattu 6.4.2015. *CodeMasters.com.*

EDGE. 2008. “Ten Most Annoying DRM Methods”. Saatavilla verkosta: <http://web.archive.org/web/20131129130447/http://www.edge-online.com/features/ten-most-annoying-drm-methods>. Viitattu 13.4.2015. *EDGE.*

Fox, B. 2003. “’Subversive’ code could kill off software piracy”. Saatavilla verkosta: <http://www.newscientist.com/article/dn4248-subversive-code-could-kill-off-software-piracy.html>. Viitattu 6.4.2015. *NewScientist.*

Gaber, T. 2013. “E-Marketing in Developed and Developing Countries: Emerging Practices”. Luku Digital Rights Management: Open Issues to Support E-Commerce, toimittanut H. El-Gohary ja R. Eid, 69–87. Pennsylvania, USA: IGI Global. ISBN: 9781466639546.

Gerardi, M., J. Teti ja D. Toal. 2013. “Caught you red-handed: 9 games with creative copy protection”. Saatavilla verkosta: <http://gameological.com/2013/05/inventory-9-games-with-creative-drm-copy-protection/>. Viitattu 13.4.2015. *The Gameological Society.*

Ghazi, K. 2012. “PC Game Piracy Examined”. Saatavilla verkosta: <http://www.tweakguides.com/Piracy_1.html>. Viitattu 31.3.2015. *TweakGuides.com.*

Grayson, N. 2011. “Interview: Bohemia Interactive’s CEO on fighting piracy, creative DRM”. Saatavilla verkosta: <http://www.pcgamer.com/interview-bohemia-interactives-ceo-on-fighting-piracy-creative-drm/>. Viitattu 6.4.2015. *PC Gamer.*

Holm, P. 2014. “Piracy on the simulated seas: the computer games industry’s non-legal approaches to fighting illegal downloads of games”. Saatavilla verkosta: <http://dx.doi.org/10.1080/13600834.2014.899770>. Viitattu 31.1.2015. *Information & Communications Technology Law* 23 (1): 61–76.

Hyams, R. 2008. *Copy Protection of Computer Games.* Saatavilla verkosta: <https://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-03.pdf>. Viitattu 20.4.2015. Royal Holloway, University of London, Surrey, Englanti.

Layton, J. 2006. “How Digital Rights Management Works”. Saatavilla verkosta: <http://computer.howstuffworks.com/drm.htm>. Viitattu 28.2.2015. *HowStuffWorks.com.*

The truth about StarForce drivers. Saatavilla verkosta: <http://www.onlinesecurity-on.com/info.phtml?c=89>. Viitattu 25.4.2015.

Plunkett, L. 2011. “Now This Is How Copy Protection Should be Done, People”. Saatavilla verkosta: <http://kotaku.com/5858150/now-this-is-how-copy-protection-should-be-done-people>. Viitattu 13.4.2015. *Kotaku.*

Rosenblatt, W., S. Mooney ja W. Trippe. 2001. *Digital Rights Management: Business and Technology.* New York, USA: John Wiley & Sons. ISBN: 9780764548895.

General information about SecuROM. Saatavilla verkosta: <https://support.securom.com/faq_general.html>. Viitattu 4.4.2015.

StarForce Disc. Saatavilla verkosta: <http://www.star-force.com/products/starforce-disc/>. Viitattu 13.4.2015.

StarForce ProActive. Saatavilla verkosta: <http://www.star-force.com/products/starforce-proactive/>. Viitattu 13.4.2015.

StarForce Products. Saatavilla verkosta: <http://www.star-force.com/products/>. Viitattu 6.4.2015.

What is Steam. Saatavilla verkosta: <http://web.archive.org/web/20080906004126/http://store.steampowered.com/about/>. Viitattu 13.4.2015.

Van Tassel, J. 2006. *Digital Rights Management: Protecting and Monetizing Content.* NAB Executive Technology Briefings. Massachusetts, USA: Focal Press. ISBN: 9780240807225.