Upravljanje digitalnim pravima na Internetu

Vukman, Vanja

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2018./2019.

Vanja Vukman

Upravljanje digitalnim pravima na Internetu

Završni rad

Mentor: dr. sc. Radovan Vrana, izv. prof.

Zagreb, srpanj 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Zahvaljujem mentoru dr. sc. Radovanu Vrani na korisnim savjetima tijekom pisanja završnog rada.

Sadržaj

1. Uvod

U današnje vrijeme teško je govoriti o svim blagodatima koje je donio razvoj digitalnih medija, a da se pritom ne dotaknemo i nekih slabosti kojima je takva vrsta medija sklona. Razvoj digitalnih medija je bez sumnje veliki korak naprijed za čovječanstvo kojim smo dosegnuli vrhunac informacijskog (digitalnog) doba. Danas je gotovo nemoguće pronaći osobu koja nije koristila neki oblik digitalnih medija od zvučnih zapisa, digitalnih fotografija i filmova pa do e-knjiga, videoigara te raznih softverskih alata. Oni su postali sastavni dio našeg društva koji nam neizmjerno olakšavaju život i poslovanje. Tome je doprinijela i lakoća njihovog korištenja i distribucije. U teoriji, na olakšanu uporabu i distribuciju digitalnih sadržaja se gleda kao na vrlo pozitivnu karakteristiku, no u praksi je to dvosjekli mač. Naime, ovu prednost mogu iskoristiti pojedinci koji nemaju dozvolu za korištenje i umnožavanje digitalnih sadržaja što se na kraju negativno odražava na autore i izdavače istih. Takvo neovlašteno korištenje i umnožavanje digitalnih sadržaja zove se piratstvo i predstavlja veliki problem njihovim autorima koji su kroz cijeli proces digitalne tranzicije pokušavali pronaći odgovor na isti. Stoga su mnogi proizvođači i distributeri razvili razne tehnologije i standarde koje bi ograničile uporabu digitalnih sadržaja te na taj način zaštitili svoja djela. Ove tehnologije i standardi se skupa nazivaju upravljanje digitalnim pravima (eng. Digital Rights Management – DRM).

Kada u cijelu tu priču uključimo i Internet, situacija postaje mnogostruko složenija. Internet korisnicima omogućava nevjerojatnu slobodu u pristupanju informacijama i digitalnim sadržajima te samim time u velikoj mjeri doprinosi rastu piratstva što zauzvrat dodatno potiče jačanje mjera za zaštitu digitalnih sadržaja. Budući da DRM štiti sadržaj na način da ograničava njegovu uporabu, takva ograničenja sadržaja postaju sve drastičnija i rigoroznija. Ovakav rasplet situacije nikako ne odgovara kupcima digitalnih sadržaja koji zapravo dobivaju manje nego što su platili.

U nastavku rada će se detaljno objasniti tehnologije i oblici zaštite koji se koriste te će se ukazati na njihove nedostatke tj. utjecaj DRM-a na uporabljivost digitalnog sadržaja poput filmova, glazbe, videoigara te e-knjiga. Prikazat će se i napredak tih tehnologija od njihovog početka pa do danas. Time će se moći vidjeti koliko su se mjere protiv piratstva postrožile, a i koliko su one u stvari uspješne.

2. O upravljanju digitalnim pravima (DRM-u)

Da bismo uopće mogli govoriti o ovoj temi, najprije je bitno definirati i objasniti što je to upravljanje digitalnim pravima, odnosno DRM[1]. Godwin (2004) definira DRM kao „kolektivno ime za tehnologije koje sprječavaju korištenje digitalnih djela zaštićenih autorskim pravima izvan okvira koje je postavio sam vlasnik autorskih prava“. Odnosno, to je naziv za više različitih tehnologija koje ograničavaju uporabu digitalnog sadržaja do određenog stupnja. Sada se postavlja pitanje zašto bi vlasnik digitalnog sadržaja uopće htio ograničiti njegovu uporabu. Odgovor je vrlo jednostavan i može se objasniti na temelju banalnog primjera. Zamislite da posudite knjigu iz knjižnice te ju date kopirati. Time kršite autorsko pravo i možete biti kazneno gonjeni, međutim, ovu radnju je moguće učiniti te je samo pitanje vaše slobodne volje hoćete li to učiniti ili nećete. DRM poništava ovu mogućnost. Za razliku od fizičke knjige, njezin digitalni ekvivalent e-knjiga se može zaštititi DRM-om te će se spriječiti mogućnost njezina kopiranja, slanja drugim osobama, posuđivanja itd. Dakle, u ovom slučaju vi nemate pravo odlučiti hoćete li počiniti kazneno djelo ili ne jer je to već u samom startu onemogućeno.

Nažalost, time se zapravo stavlja i teret na samog kupca kojem se daje mogućnost čitanja e-knjige samo na određenom uređaju i platformi. To znači da osoba koja plati e-knjigu gubi neka od prava koje bi kao kupac trebao imati. Kako se vidi iz priloženog, iz perspektive kupaca DRM nije idealno rješenje. No o tome će biti govora u daljnjim poglavljima.

Naravno, navedeni primjer se ne odnosi samo na e-knjige nego na sve sadržaje koji su digitalizirani i time lako djeljivi poput videoigara, glazbe, filmova itd. Layton (2006) smatra kako je sav sadržaj došao na nemilost DRM-a upravo zbog digitalne revolucije koja je omogućila korisnicima da koriste digitalne sadržaje na „posve nove i inovativne načine“ što vlasnicima autorskih prava otežava pa čak i onemogućava kontrolu nad distribucijom istih. Ovi posve novi i inovativni načini koje spominje nisu ništa drugo nego piratstvo te iz tog razloga Layton (2006) definira DRM kao „generalni termin koji se koristi za svaku vrstu tehnologije koja nastoji zaustaviti ili umanjiti praksu piratstva“. U svakom slučaju ovo je mnogo jednostavnija i izravnija definicija DRM-a.

[1] Kraticu DRM (Digital Rights Management) ću u nastavku rada koristiti kao zamjenu za termin upravljanje digitalnim pravima

3. Povijest DRM-a

DRM je prvotno bio razvijen da bi se zaštitio softver od kopiranja te da bi se kontrolirao pristup plaćenim TV programima na set-top box uređajima u audiovizualnoj potrošačkoj elektronici (Gaber, 2013). Zanimljivo je kako je IBM već krajem 60-ih razmišljao o primjeni takvog sustava na njihov softver, ali su na kraju odustali (Smith, 2017). Jedan od zaposlenika IBM-a Watts S. Humphrey je tada rekao kako bi to bilo „nepraktično i nezgodno za korisnike, a skupo za IBM“ (citirano u Smith, 2017). Također je dodao kako bi „bilo kakvi posebni programi s mogućnošću isključivanja ili samouništenja bili gnjavaža za vjerne korisnike i neučinkoviti protiv pametnih lopova“ (citirano u Smith, 2017). Ovakav stav su zadržali do kraja 90-ih kada su osmislili vlastitu DRM tehnologiju za zaštitu svog softvera (Smith, 2017).

Jedan od najranijih DRM sustava je bio Serial Copy Management System (SCMS) razvijen sredinom 80-ih. SCMS je sprječavao ilegalno kopiranje prve generacije digitalne tehnologije za snimanje – digitalne audio trake (DAT). Taj sustav se temeljio na kontrolnim bitovima koji su određivali mogućnost kopiranje DAT kaseta na DAT snimačima (Gaber, 2013). SCMS se pokazao kao vrlo nedjelotvoran sustav zbog mnogih mogućnosti zaobilaska zaštite.

Tek 90-ih su počeli nastajati DRM sustavi kakve danas poznajemo, a koji se mogu podijeliti u dvije generacije. Prva generacija je bila fokusirana na sigurnost i enkripciju kako bi se sprječilo neautorizirano kopiranje (Ianella, 2001). Današnja, druga generacija uz enkripciju pokriva zaštitu, opis, identifikaciju, trgovinu, nadzor te praćenje svih vrsta prava korištenja nad digitalnim sadržajima (Ianella, 2001).

3.1. Prva generacija DRM sustava

Prva generacija DRM sustava je koristila razne enkripcijske tehnike koje su digitalni sadržaj vezale uz samo jedan uređaj (Gaber, 2013). To je značilo da potrošač nije mogao dijeliti sadržaj s drugima. On je mogao raditi kopije i distribuirati ih, ali su primatelji tih kopija trebali novi dekripcijski ključ (Gaber, 2013). Drugim riječima, to je značilo da su primatelji kopiranog sadržaja trebali kontaktirati izdavača licenci kako bi nabavili enkripcijski ključ koji bi im omogućio korištenje sadržaja (Gaber, 2013). Jedan poznati primjer DRM sustava prve generacije je InterTrustov Digibox. Taj sustav je omogućavao distribuciju digitalnog sadržaja

preko otvorenih kanala (Nelson, 2001). Da bi se to postiglo, Digibox sustavi kombiniraju digitalni sadržaj s „kontrolama“ za upravljanje pravima u zaštićenom spremniku (Nelson, 2001). Ovakvim zaštićenim spremnicima su imali pristup samo autorizirani korisnici.

3.2. Druga generacija DRM sustava

Razlog nastajanja druge generacije DRM sustava bio je rapidan razvoj Interneta krajem 90-ih (Gaber, 2013). Kao što je bilo ranije spomenuto, Internet je potaknuo povećanje piratstva pa su se samim time morale poduzeti i odgovarajuće mjere. Da budemo precizniji, trebalo je doći do rješenja koji će kontrolirati korištenje digitalnog sadržaja poslije njegove distribucije (Gaber, 2013). Stoga se druga generacija DRM sustava uz enkripciju sadržaja fokusira i na kontrolu pregledavanja, kopiranja, printanja, mijenjanja te svega ostaloga što je moguće učiniti s digitalnim sadržajima (Layton, 2006).

DRM sustavi ove generacije su nam već malo poznatiji jer ih susrećemo gotovo svakodnevno. Potrošačima je u ovoj generaciji omogućeno korištenje sadržaja na više od jednog uređaja te njihovo dijeljenje s prijateljima ili obitelji što je moguće kroz koncept autorizirane domene (Gaber, 2013). Neki poznatiji DRM sustavi ove generacije su Appleov FairPlay, Google Widevine, Denuvo itd. Oni će biti detaljnije objašnjeni u kasnijim poglavljima.

4. Načelo rada DRM-a

4.1. Digitalni sadržaj i licenca

Da bi se objasnio rad DRM-a potrebno je prvo definirati neke pojmove i procese. Osnovni koncept koji moramo razumjeti kod DRM sustava jest da postoje dva razdvojena entiteta, a to su digitalni sadržaj i licenca (Gaber, 2013). Sam sadržaj je izvor prihoda kod digitalnog sadržaja koji nema DRM, dok je kod digitalnog sadržaja s DRM-om izvor prihoda licenca. Dakle, prije nego se sadržaj pošalje potrošaču on se kriptira pomoću simetričnog ključa Content Encryption/Decryption Key (CEDK). Zatim se zaštićeni sadržaj šalje potrošaču koji za otvaranje tog sadržaja treba kupiti odgovarajuću licencu (Gaber, 2013).

Digitalni sadržaj zaštićen DRM-om je digitalna datoteka koja sadrži kriptirani sadržaj i sljedeće objekte:

- Jedinstveni identifikator (eng. Unique identifier) za taj kriptirani sadržaj pomoću kojeg se sadržaj povezuje s pripadajućim pravima za korištenje
- Informacije o kriptirajućem algoritmu koji se koristio
- Informacije o izdavaču licence za pripadajući DRM sadržaj (Gaber, 2013).

Licenca je XML datoteka koja je generirana da opiše prava za korištenje digitalnog sadržaja koji je zaštićen DRM-om (Gaber, 2013). Tipična datoteka licence sadrži prava za korištenje, CEDK, metapodatke te potpis izdavatelja licence (Gaber, 2013). Prava za korištenje (eng. Usage rights) predstavljaju skup prava koja potrošač može prakticirati sa svojim digitalnim sadržajem. CEDK je simetrični ključ koji se koristi za kriptiranje i dekriptiranje pripadajućeg digitalnog sadržaja, a potpis izdavatelja licence je digitalni potpis kojeg je generirao izdavatelj licence na datoteki licence da se zaštiti njen integritet i dokaže autentičnost (Gaber, 2013). Datoteka s metapodacima sadrži sljedeća polja:

- ID licence: jedinstveni serijski broj licence;
- ID sadržaja: jedinstveni identifikacijski broj sadržaja;
- ID davatelja sadržaja: jedinstveni identifikacijski broj izdavatelja sadržaja;
- URL preko kojeg se može dobiti licenca;
- Kriptografski parametri (Gaber, 2013)

4.2. Funkcionalni entiteti

Sada kada su se definirala dva osnovna entiteta potrebno je definirati i funkcionalne entitete. Funkcionalni entiteti su oni entiteti koji imaju određenu funkciju u cjelokupnom procesu zaštite digitalnog sadržaja. Ti entiteti su najčešće:

- **DRM Agent** koji je odgovoran za provođenje dozvola i ograničenja povezanih s DRM sadržajem, kontrolu pristupa DRM sadržaju itd.;
- **Davatelj sadržaja** koji isporučuje DRM sadržaj;
- **Izdavatelj prava** koji dodjeljuje dozvole i ograničenja DRM sadržaju preko generirane licence;
- **Korisnik** koji se služi DRM sadržajem, a kojem pristup može dobiti samo preko DRM Agenta (OMA-DRM-V2.0.1, 2008)

Valja napomenuti kako postoje različita imena za određene entitete pa tako neki autori entitet izdavatelj prava nazivaju izdavatelj licenci, entitet korisnik nazivaju potrošač itd.

4.3. Način rada DRM sustava

U ovom potpoglavlju će se naposljetku objasniti i rad tipičnog DRM sustava. Naravno, to ne znači da svaki sustav funkcionira na isti način budući da svaka vrsta sadržaja zahtjeva različita riješenja. Međutim, važno je dati neku predodžbu o kakvom je procesu riječ.

Sve počinje vlasnikom sadržaja koji kriptira sadržaj CEDK ključem, generira njegove metapodatke te definira prava korištenja (Gaber, 2013). Nakon toga se sadržaj i njegovi metapodaci skupa pakiraju i šalju davatelju sadržaja, dok se prava korištenja šalju izdavatelju licenci/prava (Gaber, 2013). Davatelj sadržaja zatim odlučuje koje će metode u distribuciji sadržaja koristiti, dok izdavatelj licenci mora prava korištenja pretvoriti u licencni oblik (Gaber, 2013).

Korisnik/potrošač koji želi kupiti određeni sadržaj zaštićen DRM-om dobavlja ga najčešće preko web kataloga ili DVD-a, ovisno o načinu distribucije za kojeg se davatelj sadržaja odlučio. Međutim, da bi dobio pristup sadržaju, korisnik treba instalirati DRM klijenta/agenta na svom uređaju te kupiti pripadajuću licencu od izdavatelja licenci (Gaber, 2013). Za dobivanje licence korisnik mora obaviti naplatu preko naplatnog sustava (eng.

Payment gateway) te se korisnikovom DRM klijentu mora provjeriti autentičnost na poslužitelju izdavatelja licence (Gaber, 2013). Autorizacija se vrši putem klijentovog certifikata koji sadrži informacije poput proizvođača, verzije softvera, serijskog broja itd. (OMA-DRM-V2.0.1, 2008). Nakon uspješne naplate i autorizacije, izdavatelj licence generira i potpisuje licencu. Ta licenca se zatim kriptira javnim ključem DRM klijenta i šalje korisnikovom DRM klijentu koji po njezinom primitku provjerava njezin potpis kako bi utvrdio da ju je izdao autentičan izdavač licenci (Gaber, 2013). Klijent zatim dekriptira licencu uz pomoć privatnog ključa te iz nje izvlači CEDK kojim naposljetku dekriptira cjelokupan sadržaj (Gaber, 2013). Sadržaj je tada spreman za upotrebu.

5. Oblici zaštite digitalnih sadržaja

U ovom poglavlju će se navesti i opisati neki od najpoznatijih DRM oblika za sljedeće digitalne sadržaje: videoigre, filmove, glazbu i e-knjige. Isto tako će se uz objašnjenja dati i neki primjeri koji pokazuju koliko su spomenute tehnologije zapravo učinkovite i dobre za kupce.

5.1. Videoigre

Videoigre su od svojih početaka u drugoj polovici 20. st. pa do danas postale jedna od najunosnijih grana u IT industriji. Timothy O'Shea, analitičar koji se bavi sektorom za videoigre, je rekao da „gaming otima tržišni udio ostalim oblicima medija“ pa dodaje kako “raste brže od filmova i TV-a“ (Ell, 2018). Najbolji dokaz za ovo je rast nagradnog fonda za jednu od najpopularnijih kompetitivnih igara današnjice – Dote 2. U 2018. je nagradni fond za The International (najveći turnir u Doti 2) iznosio 24,8 milijuna dolara (Makuch, 2018). S jačanjem popularnosti ostalih igara poput Fortnite-a i Apex Legendsa predviđa se da će u budućnosti na tron zasjesti neka druga igra s mnogo većim nagradnim fondom koji ionako iz godine u godinu drastično raste (Makuch, 2018). No to su nagradni fondovi za igrače, zarada za proizvođače je mnogo veća. Tako Valve, proizvođač Dote, zaradi toliko svakih mjesec dana, dok Riot Games, proizvođač igre League of Legends koja je Dotin najveći rival, zaradi isti iznos za samo 5 dana (Grubb, 2019). Predviđa se da će do 2020. godine globalno tržište videoigara vrijediti 128,5 milijardi dolara (Taylor, 2018).

Iz ovih primjera se vidi kolika je zapravo važnost videoigara i koliko se resursa posvećuje njezinom daljnjem rastu. Dota 2, League of Legends i Fortnite su u ovom slučaju besplatne igre što znači da njihovi proizvođači ne zarađuju niti približno koliko zarađuju oni koji prodaju svoje igre. Zarada jednog takvog giganta poput Electronic Artsa je u prošloj godini bila oko 5 milijardi dolara (Duran, 2019). Stoga ne čudi činjenica da mnoge kompanije čine sve da zaštite svoj sadržaj i ostvare maksimalan profit. EA je po tom pitanju česta meta kritika koje se tiču njihove DRM politike. Naime, EA je već dugo vremena najomraženija kompanija u svijetu videoigara, a sve je započelo s pretjeranom primjenom ograničavajućih mjera na videoigri Spore 2008. godine. Tehnologija koja se tada koristila zvala se SecuROM. Doduše, ona se danas više ne koristi, ali su je zamijenili još zloglasniji oblici zaštite poput Denuvo Anti-Tampera te always-online DRM-a. SecuROM, Denuvo i always-online DRM će se detaljnije objasniti u nastavku.

5.1.1. Oblici zaštite videoigara

5.1.1.1. SecuROM

SecuROM se koristio u različitim oblicima od videoigara poput Diabla 2, Alien vs. Predatora 2, Unreal Tournamenta 2004 pa do Bioshocka, Crysisa i Grand Theft Auta 4. To je bila vrlo popularna DRM tehnologija koju je razvio Sony Digital Audio Disc Corporation, a koja se prestala koristiti u prvoj polovici ovog desetljeća. Međutim, neke igre iz tog razdoblja su još uvijek zaštićene ovom tehnologijom.

SecuROM je funkcionirao na način da je provjeravao gustoću podataka koji su se čitali s diska (Smith, n.d.). Gustoća podataka pada od unutrašnjosti DVD-a prema van, a SecuROM dopušta distributerima da se toj degradaciji podataka doda poseban uzorak (Smith, n.d). Ako prilikom pokretanja taj uzorak nije nađen, igra neće moći raditi jer će SecuROM utvrditi da DVD nije važeći (Smith, n.d.). Stoga je DVD trebao uvijek biti u optičkom uređaju iako je igra možda bila instalirana na računalo. To je prvi veliki problem SecuROM-a, a biti će ih još i više. Naime, glavni razlog zašto je SecuROM izdržao toliko dugo u industriji je taj što je to modularan program i razni proizvođači i izdavači su na njega mogli vezati dodatne vlastite mjere zaštite (Smith, n.d.). Te mjere zaštite su uglavnom uključivale online aktivaciju videoigara te ograničenje broja mogućih aktivacija neke igre po kupljenom proizvodu.

Upravo to je bilo sporno u slučaju Electronic Artsa i njihove videigre Spore. Naime, EA je preko SecuROM-a ograničavao korisnike na samo 3 moguće aktivacije po kupljenom proizvodu (Alexander, 2008). To je značilo da korisnici koji su kupili igru je nisu mogli instalirati na više od 3 uređaja. Isto tako to je značilo da se na istom uređaju igra nije mogla instalirati više od 3 puta što je bilo izuzetno nepošteno prema kupcima. Ovakvim pristupom su zapravo sve kupce tretirali kao potencijalne lopove. Iz Electronic Artsa su poručili kako u tome ne vide ništa sporno te kako je samo 1% kupaca pokušalo aktivirati igru na više od 3 uređaja (Alexander, 2008). Međutim, ono što je najgore je to da je Spore bio relativno brzo piratiziran unatoč SecuROM-u pa su jedini gubitnici u cijeloj toj priči bili oni koji su ga kupili. Ubrzo su slijedile tužbe protiv Electronic Artsa u kojima je bilo navedeno da kupci nisu znali da će se instalacijom videoigre instalirati poseban odvojeni program koji će biti u mogućnosti izvoditi vlastite operacije (Guevin, 2009). Nije dokazano da je SecuROM bio rootkit, međutim bilo je slučajeva gdje je SecuROM ugrozio stabilnost računala (Smith, n.d.). Tako su, primjerice, igrači kod instalacije videoigre The Sims 2 primjetili da je SecuROM onesposobio

neke od njihovih računalnih programa te da je ometao rad antivirusnih programa (Smith, n.d.).

5.1.1.2. Always-online DRM

Always-online DRM je do nedavno bila vrlo korištena metoda kod zaštite videoigara. To je oblik zaštite koji prisiljava igrače da budu cijelo vrijeme povezani na Internet tijekom igranja određene igre. Ono što je bitno istaknuti ovdje jest da igre zaštićene ovim oblikom DRM-a ne trebaju nužno biti igre za više igrača (eng. multiplayer) koje se ionako igraju preko interneta nego mogu biti i igre za jednog igrača (eng. singleplayer) kojima nije potrebna povezanost na Internet da bi se igrale. Dakle, ukoliko igra izgubi vezu sa poslužiteljem, a to se najčešće događa zbog spore brzine Interneta ili gubitka povezanosti s istim, ona prestaje raditi. Ovakva vrsta zaštite zapravo narušava doživljaj igranja videoigre te ograničava korisnika. Kupac u ovom slučaju plaća poluproizvod jer ga ne može uvijek koristiti. Isto tako, neki poslužitelji za videoigre neće uvijek biti u funkciji pa samim time niti videoigra neće moći raditi. Jedan ekstremni slučaj se ponovno može naći kod videoigre koju je izdao Electronic Arts – Darkspore. To je nasljednik kontroverzne igre Spore koja je bila spomenuta u prošlom potpoglavlju. Kako je ta igra zbog svoje always-online DRM zaštite bila ovisna o poslužiteljima Electronic Artsa, ona nije mogla funkcionirati bez njih (Richard, 2016). Naravno, poslužitelji ne mogu vječno podržavati neku videoigru i s vremenom se oni moraju ugasiti. No u ovom slučaju njihov prekid rada je zapravo onemogućio igranje te igre. Svaka kopija Darkspore-a ikada kupljena postala je trajno neupotrebljiva (Richard, 2016). Stoga se može reći da always-online DRM stavlja rok trajanja na igre koje bi trebao zaštititi. Zanimljivo, ni u tome nije veoma uspješan budući da je piratsku verziju Darkspore-a još uvijek moguće naći i zaigrati. Isto tako, pojedinci koji posjeduju piratiziranu verziju igara zaštićenih always-online DRM-om mogu lagodnije igrati iste.

Danas proizvođači i izdavači videoigara polako odustaju od ovakve prakse upravo zbog nezadovoljstva kupaca. Stephanie Peroti (citirano iz Karmali, 2012), jedna od direktorica Ubisofta, je rekla da su ukinuli implementaciju ovog oblik DRM-a te da će za njihove buduće igre biti potrebna samo online aktivacija kod prvog korištenja. Square Enix je nedavno pustio update za njihovu igru Final Fantasy X koji je implementirao always-online DRM gotovo 3 godine nakon što je igra izašla (Khan, 2019). Nakon što su se korisnici pobunili, iz Square

Enixa su se ispričali korisnicima te obećali da će ukloniti always-online DRM u sljedećem updateu (Khan, 2019).

5.1.1.3. Denuvo Anti-Tamper

Kako ostali oblici DRM zaštite slabe tako Denuvo Anti-Tamper sve više uzima maha. Danas je to nazastupljenije DRM rješenje za videoigre, a ujedno među i najomraženijima. Osmislila ga je austrijska kompanija istog imena 2014. koja je od 2018. godine dio softverskog diva Irdeto (Taylor, 2018). Svaki proizvođač videoigara može kupiti licencu ovog softvera i integrirati ga u svoju igru (Hoffman, 2018). Dizajniran je tako da oteža krekiranje (eng. crack) igara te za razliku od prethodna dva oblika DRM zaštite u tome u većoj mjeri i uspijeva (Hoffman, 2018). Iz Denuva kažu kako softver „sprječava debugiranje (eng. debugging), obrnuti inženjering te mijenjanje izvršnih datoteka (eng. executable file)“ koji je potreban u krekiranju igara (citirano iz Purchese, 2014). Međutim, u Denuvu znaju da to neće spriječiti piratizaciju igara, pa im je cilj otežavanje i odugovlačenje procesa krekiranja (Hoffman, 2018). Time zapravo tjeraju korisnike koji ne žele čekati pojavu cracka da kupe igru (Hoffman, 2018). Također, sa svakom novo igrom postaju bolji u njezinoj zaštiti. Iz Denuva objašnjavaju kako je za probijanje zaštite na FIFA-i 13 trebalo 13 dana dok je za FIFA-u 14 trebalo 46 dana (citirano iz Purchese, 2014). Assassin's Creed: Origins iz 2017. je, primjerice, bio krekiran tek nakon 99 dana (Hoffman, 2018). No, čini se kako to i nije pravilo. Tako je, primjerice, u 2019. Rage 2 bio krekiran na dan izlaska što nikako ne ide u prilog Denuvu koji se hvale da štite igru od prebrzog piratiziranja (Fenlon 2019). Još neke igre u 2019. koje koriste Denuvo, a kojima je zaštita probijena u manje od tjedan dana su Metro Exodus (4 dana), Resident Evil 2 (6 dana), Far Cry New Dawn (6 dana) (Fenlon 2019).

Za razliku od SecuROM-a, Denuvo nije odvojeni softver koji se instalira na računalo već je integriran u sam kod videoigre (Hoffman, 2018). Ipak to ne znači da je softver bez mana. Kao i ostali DRM oblici, Denuvo ne stvara samo probleme piratima već i onima koji kupuju proizvod. Naime, zbog opterećivanja procesora Denuvo pogoršava performanse videoigara te osjetno smanjuje broj FPS-a (frames per second, hrv. sličica po sekundi). Zbog toga se neki proizvođači i izdavači igara odlučuju na njegovo uklanjanje nakon što se piratizirane igra mogu naći na Internetu. Tako su Bethesda i Arkane Studios uklonili Denuvo sa svoje igre Dishonored 2 dvije godine nakon što je izašla (Papadopoulos 2018). S druge strane, Katsuhiro Harada, jedan od direktora Bandai Namcoa, je optužio Denuvo da je

odgovoran za pad FPS-a na njihovoj PC verziji igre Tekken 7 (citirano iz Palumba, 2018). Hoffman (2018) tvrdi da su se performanse igara nakon uklanjanja Denuva poboljšale za 50%.

5.1.2. Steam

Zasigurno jedno od najpoznatijih imena u industriji videoigara je Steam. Steam je razvio Valve Corporation 2003. i od onda je izrastao u najveću platformu za digitalnu distribuciju videoigara (Klappenbach, 2017). Osim toga što omogućuje kupnju i preuzimanje igara, Steam se može pohvaliti i rastućom korisničkom zajednicom te svojom platformom za igranje koja broji više od milijun korisnika u bilo koje doba dana (Klappenbach, 2017).

Ono što je bitno reći o Steamu jest da je to ujedno i DRM sustav. Stoga je za pokretanje mnogih igara na Steamu potrebno prvo pokrenuti Steam. Također, sve igre koje korisnik kupi su vezane na njegov korisnički račun i ne mogu se u isto vrijeme igrati na dva računala preko istog korisničkog računa. Naravno, neke igre nisu obuhvaćene Steamovim DRM-om na zahtjev njezinih proizvođača. Jedan od takvih proizvođača je švedska kompanija Paradox Interactive koja javno kritizira DRM (Mendez, 2017). Sve njihove igre se mogu igrati bez pokretanja Steama te na više računala u isto vrijeme. Međutim, Mendez (2017) ističe kako je Steam općenito vrlo blag DRM sustav, stoga su i ovakvi pozitivni primjeri na Steamu prilično neprimjetni. Korisnik, primjerice, ne treba cijelo vrijeme biti povezan na Internet, a autentifikacija se izvršava svaka dva tjedna (Mendez, 2017). Steam u svojoj DRM zaštiti koristi Custom Executable Generation tehnologiju (Alexander, 2009). Kada se preuzme videoigra zaštićena ovom tehnologijom korisnik u stvari dobije dvije komponente (Demerjian, 2009). Prva komponenta je cijela nepromijenjena videoigra sa svim njezinim podacima te zvučnim i grafičkim datotekama dok je druga komponenta izmijenjena izvršna datoteka čija je veličina samo nekoliko megabajta (Demerjian, 2009). Svaka takva izvršna datoteka je kriptirana na jedinstven način i vezana za određeni korisnički račun (Demerjian, 2009). Samo korisnički račun koji je povezan s tom izvršnom datotekom je može dekriptirati i pokrenuti videoigru (Demerjian 2009). To omogućava višestruku instalaciju na više računala no ključ će se povući samo kada je korisnik ulogiran na Steam (Demerjian, 2009). Kada se sljedeći korisnik ulogira na svoj korisnički račun preuzet će se samo izvršna datoteka od nekoliko megabajta umjesto cijele videoigre (Demerjian, 2009).

Uz standardnu CEG tehnologiju, Steam podržava i DRM tehnologije treće strane. Prethodno objašnjeni SecuROM i always-online se tako mogu naći na nekim od igara, dok je Denuvo Anti-Tamper najčešća tehnologija treće strane koja se danas koristi na igrama na Steamu.

5.2. Filmovi

Filmovi su daleko najpiratiziraniji digitalni sadržaj na Internetu. To nije ništa čudno budući da je film ujedno i najpopularniji medij već dugi niz godina. Filmska industrija je u 2018. ostvarila prihod od 136 miljardi dolara što je više od ostalih medija, a taj prihod nastavlja rasti iz godine u godinu (ibisworld.com, 2018). Unatoč tome, u filmskoj industriji su svjesni gubitaka koje im piratstvo donosi svake godine pa ga stoga ni najmanje ne toleriraju. Ipak pojava streaming servisa poput Netflixa, HBO Go-a te Amazon Primea je na neki način zaustavila trend rasta piratstva. Naime, ovi servisi nude veliki izbor filmova i serija u vrhunskoj kvaliteti slike i to po vrlo povoljnoj cijeni što ljude zapravo odvraća od piratstva. Može se reći da je ovakav OTT (over-the-top) način distribucije zamijenio onaj standardni način preko fizičkih medija.

5.2.1. Oblici zaštite filmova

Neke od poznatijih DRM tehnologija za zaštitu filmova kod standardnog načina distribucije su: CSS (eng. Content Scramble System) i AACS (eng. Advanced Access Content System). CSS se koristio u zaštiti svih DVD-video diskova, ali se pokazao vrlo ranjiv pa je kasnije zamijenjen boljim DRM rješenjima poput AACS-a (CARNet, 2007). AACS se koristio za zaštitu optičkih diskova nove generacije poput HD DVD-a i Blu-ray diskova te se temeljio na kriptiranju sadržaja (CARNet, 2007). Ove tehnologije se neće detaljnije opisati upravo zbog činjenice da su štitile sadržaj koji se distribuirao preko fizičkih medija, a ne Interneta. Međutim važno ih je spomenuti jer su itekako važne za daljnji razvoj DRM rješenja.

DRM tehnologije o kojima će biti govora u nastavku su rješenja za spomenute OTT servise poput Netflixa i Amazon Prime-a, a koja će funkcionirati na uređajima koji podržavaju ove servise. To uključuje HTML5 preglednike poput Firefoxa i Chrome-a, mobilne uređaje s iOS ili Android operativnim sustavima, različite Smart TV uređaje te konzole poput Xboxa i Playstationa (vixyvideo.com, 2018). Djelovanje ovih rješenja se može podijeliti u sljedeća 4 koraka:

1. Izvorna datoteka filma se stavlja na OTT platformu;
2. Sustav za kodiranje video zapisa počet će kodirati izvorne datoteke u prilagodljive streaming formate kao što su MPEG-Dash ili HLS, a enkoder će šifrirati datoteke s medijskim ključevima jednog ili više davatelja DRM-a;
3. Kodirane i enkriptirane datoteke se premještaju u spremište ili Content Delivery Network (CDN) te su spremne da ih pokrene autorizirani krajnji korisnik;
4. Krajnji korisnik pokreće film te video player počinje komunicirati sa poslužiteljem da provjeri autentičnost licence. Kada proces autentifikacije završi, video player dekriptira film i počinje ga emitirati (vixyvideo.com, 2018)

Rješenja o kojima će biti govora u nastavku su: Google Widevine i Microsoft PlayReady.

5.2.1.1. Google Widevine

Google Widevine je Googleovo DRM rješenje koje omogućuje stvarateljima sadržaja da streamaju zaštićeni sadržaj (vdocipher.com, n.d.a). Primjerice, brojni OTT servisi poput Netflixa i Amazon Primea ne dozvoljavaju nekim smarthphone uređajima da streamaju filmove ili serije u rezoluciji većoj od 480p (Triggs, 2019). Razlog tome je što se ovi servisi na taj način štite od kopiranja i neautorizirane distribucije video datoteka (Triggs, 2019). Da bi smartphone uređaji mogli streamati filmove i serije u većoj rezoluciji, streaming servisi im moraju vjerovati da su sigurni od piratstva (Triggs, 2019). Takvo povjerenje se dobiva upravo preko Google Widevine DRM platforme koja je implementirana na mnogim smartphone uređajima (Triggs, 2019). Na računalima Widewine DRM podržavaju web preglednici poput Chrome-a, Firefoxa i Opere (vdocipher.com, n.d.a).

Google Widevine radi tako da implementira mnoge standarde u svrhu zaštite sadržaja prilikom njegova transfera preko Interneta pa do pokretanja na uređajima (Triggs, 2019). On koristi kombinaciju CENC enkripcije (Common Encryption Scheme), izmjene ključeva te adaptabilne streaming kvalitete za upravljanje i slanje videa krajnjim korisnicima (Triggs, 2019). CENC osigurava da je svaki segment videa kriptiran samo jednom (vdocipher.com, n.d.a). Triggs (2019) objašnjava kako je ideja olakšati posao streaming servisima budući da platforma podržava različite razine streaming kvalitete ovisno o sigurnosnim sposobnostima uređaja koji prima sadržaj. Stoga Widevine štiti sadržaj preko tri razine sigurnosti, a to su: L1,

L2 i L3. Svaki korisnik koji želi streamati HD sadržaj preko servisa poput Netflixa mora imati uređaj koji ima L1 certifikat (Triggs, 2019). Za L1, svako procesiranje i dekriptiranje sadržaja se mora izvoditi u Trusted Execution Environmentu (TEE) procesora na uređaju da se izbjegne vanjsko kopiranje sadržaja (Triggs, 2019). Kod L2 se dekriptiranje sadržaja može izvoditi izvan TEE-a, ali ne i procesiranje sadržaja (Triggs, 2019). L3 se primjenjuje kada uređaj nema TEE ili kada se procesiranje sadržaja izvodi izvan (Triggs, 2019).

Android uređaji podržavaju ili L1 ili L3 sigurnosnu razinu ovisno o softveru i hardveru dok preglednici poput Chrome-a na desktopu podržavaju samo L3 (Triggs, 2019). Dakle, ako gledate Netflix na računalnoj verziji Chrome-a ili Firefoxa ne možete dobiti kvalitetu slike veću od 720p čak i ako plaćate tu opciju.

5.2.1.2. Microsoft Playready

Microsoft Playready je Microsoftovo DRM rješenje koje omogućuje stvarateljima i distributerima sadržaja da streamaju zaštićeni sadržaj (vdocipher.com, n.d.b). Playready je uglavnom podržan na uređajima i softveru koji pokreću Microsoftove preglednike poput Edge-a i Internet Explorera (vdocipher.com, n.d.b).

Microsoft Playready nudi dvije bitne mogućnosti za zaštitu digitalnog sadržaja. Prva mogućnost je sprječavanje preuzimanje sirovog videa preko sigurnog mehanizma kriptirane reprodukcije (vdocipher.com, n.d.b). Druga mogućnost je zabrana korištenja alata za snimanje zaslona na razini hardvera (vdocipher.com, n.d.b). Dakle, ukoliko se gleda neki film na Netflixu preko Microsoft Edge-a, taj film se neće moći snimiti preko alata za snimanje ekrana. No, zbog bolje zaštite, Netflix se može gledati na Microsoftovim web preglednicima u puno boljoj kvaliteti. Edge je tako jedini web preglednik na kojem se Netflix može gledati u 4K rezoluciji (Hachman, 2017). Naravno, zaobilasci zaštite su uvijek mogući što se pokazalo kod gotovo svakog DRM rješenja.

Također, Microsoft Playready, baš kao i Google Widevine, štiti sadržaj preko tri razine sigurnosti. Budući da su u tom pogledu gotovo identični te da se uglavnom razlikuju u web preglednicima i uređajima na kojima djeluju, Microsoft Playready se neće detaljnije objašnjavati.

5.2.1.3. High Bandwidth Content Protection

High Bandwidth Content Protection je još jedan oblik zaštite digitalnih video sadržaja. Iako tehnički to nije oblik DRM-a, veoma je srodan i bilo bi ga dobro spomenuti u kontekstu zaštite sadržaja. Također, danas je to jedna od bitnijih stavki na koju se mora paziti kod kupnje novih televizora ili monitora. Naime, on štiti digitalni sadržaj kod njegovog prijenosa s nekog uređaja na TV kroz HDMI ili DVI kablove. Da bi se sadržaj reproducirao bez greške, televizor i uređaj koji reproducira sadržaj moraju podržavati HDCP. Danas više manje svaki uređaj podržava HDCP no problem je taj što će se možda razlikovati u verzijama. Nova generacija HDCP-a 2.2 nije kompatibilna sa starijima i mnogi 4K uređaji je ne podržavaju (Morrison, 2014). Dakle, ukoliko se kupi televizor ili monitor koji ne podržava HDCP 2.2, mnogi 4K digitalni sadržaji se neće moći reproducirati u toj rezoluciji.

HDCP nije DRM jer ga ne brine kakav sadržaj se prenosi već isključivo sigurnost prijenosa (Morrison, 2014). Prijenos osigurava izradom kriptiranih ključeva između izvora i zaslona (Morrison, 2014). Da bi došlo do prijenosa sadržaja, izvor i zaslon se moraju slagati, a to se događa ako razumiju ključeve među sobom (Morrison, 2014). To se zove HDCP „rukovanje“ i upravo je „rukovanje“ najčešći korijen problema ako se video ne želi reproducirati ili se reproducira u slabijoj kvaliteti (Morrison, 2014).

5.3. Glazba

Baš kao i kod filmova, piratizacija glazbe se smanjila zbog pojave streaming platforma poput Spotifyja i Deezera. Ne može se očekivati da će se u doba Interneta glazba naplaćivati isto kao i u doba kada ga nije bilo. Stoga streaming servisi nude vrlo povoljne cijene za slušanje bilo koje pjesme neograničeni broj puta što je veoma isplativo. Međutim i kupovanje glazbenog sadržaja preko Interneta je još uvijek veoma popularno budući da se cijene cijelih albuma kreću oko 10 dolara (Bott, 2010). Također, mnogi servisi koji nude kupovinu glazbe preko Interneta su odustali od implementacije DRM-a na iste. Primjerice, Appleov FairPlay DRM se od 2009. više ne koristi za prevenciju kopiranja pjesama i albuma kupljenih na iTunesu (Harris, 2019a). Razlog tome se krije u Steve Jobsovom članku „Thoughts on Music“ iz 2007. u kojem je dao svoje mišljenje o DRM-u i njegovoj primjeni na glazbu (macdailynews.com, 2007). Jobs (citirano iz macdailynews.com, 2007) je tada napisao kako „DRM nije nikada funkcionirao, a vjerojatno niti nikada neće funkcionirati u

zaustavljanju piratizacije glazbe“. Stoga se zalagao za model prodaje glazbe bez DRM-a (citirano iz macdailynews.com, 2007).

5.3.1. Napster

Priča s distribucijom glazbe preko Interneta i kršenja autorskih prava počela je još 1999. s pojavom jedne vrlo kontroverzne platforme znane kao Napster. Napster je bio P2P servis za dijeljenje datoteka kojeg su osmislili Shawn Fanning i Sean Parker. Softver je bio jednostavan i korisnici su za njegovu uporabu trebali imati samo korisnički račun koji je bio besplatan (Harris, 2019b). Napster je omogućavao dijeljenje digitalnih glazbenih datoteka u MP3 formatu preko Interneta (Harris, 2019b). Servis je brzo postao veoma popularan te je u jednom trenutku imao čak 80 milijuna korisnika (Harris, 2019b). No iako nijedna MP3 datoteka nije bila pohranjena na nekim od Napsterovih poslužitelja budući da su korisnici preuzimali datoteke jedni od drugih, Napster je ubrzo postao meta RIAA-e (Recording Industry Association of America) (Lamont, 2013). RIAA je podnijela tužbu protiv Napstera zbog neautorizirane distribucije sadržaja zaštićenim autorskim pravima tvrdeći da Napster nije imao nikakvu kontrolu nad prijenosom zaštićenih materijala na svojoj mreži (Harris, 2019b). Naposljetku, Napster se 2001. morao ugasiti, a sudski sporovi su trajali i dugo nakon toga (Lamont, 2013).

Unatoč neslavnom padu platforme, može se reći da je Napster utabao put mnogim drugim servisima poput iTunesa koji sadrži i neke njegove elemente (Lamont, 2013). Plaćanje i DRM zaštita, naravno, nisu bili jedni od njih. Ipak, kako se objasnilo u prethodnom poglavlju, DRM je naposljetku uklonjen, a vodeću riječ u digitalnoj distribuciji glazbe je preuzeo Spotify čijem je rastu pridonio i sam Sean Parker (Lamont, 2013).

5.3.2. Analogna rupa

Jedan od glavnih razloga zašto se odustaje od DRM zaštite na digitalnim glazbenim sadržajima jest analogna rupa. Budući da se svaki digitalni signal mora pretvoriti u analogni kako bi ga korisnik mogao konzumirati, moguće je taj analogni signal i snimiti (CARNet, 2007). Korisnik može s tako snimljenim sadržajem raditi što god želi budući da on nije zaštićen DRM-om te se stoga nikakva ograničenja u distribuciji ne primjenjuju na njega (CARNet, 2017). Dakle, analogna rupa je slabost DRM-a kod sadržaja poput videa i glazbe. Budući da su videi snimljeni na taj način puno lošije kvalitete, može se reći da je DRM kod

glazbe jedini primjer gdje se ta slabost može sasvim iskoristiti. Sicker, Ohm i Gunaji (2007) su u svojem istraživanju došli do zaključka da je glazbu vrlo lako snimiti preko analogne rupe i to u odličnoj kvaliteti. Za snimanje su koristili laptop, softver GoldWave, bolje zvučnike i mikrofon (Sicker et al., 2007). Koristeći računalo su na zvučnicima reproducirali glazbu zaštićenu DRM-om koja se zatim snimila mikrofonom preko „zračne rupe“ i spremila na isto računalo (Sicker et al., 2007). Naposljetku, GoldWaveom su reducirali pozadinsku buku (Sicker et al., 2007). Ovo istraživanje nam govori koliko je DRM zapravo beskoristan i zašto se odustaje od njegove implementacije na glazbene sadržaje. Ona zapravo šteti samo onima koji su taj isti sadržaj preuzeli na legalan način.

5.4. E-knjige

Posljednji digitalni sadržaj koji će se obraditi u ovom radu, a podliježe DRM zaštiti jest e-knjiga. E-knjiga je digitalni oblik knjige koji se može čitati na računalu, pametnim telefonima, tabletima i posebnim uređajima namijenjenim za čitanje e-knjiga poput Amazonovog Kindlea (Corson-Knowles, n.d.). Svojom praktičnošću su vrlo brzo osvojile korisnike, a zbog ubrzane digitalizacije te širenja elektroničke trgovine na Internetu, nagađalo se da će zamijeniti one fizičke. Međutim, događa se nešto sasvim suprotno. Prema statistikama, u prvih 9 mjeseci 2018. fizičke knjige su generirale prihode od 4 milijarde dolara, dok su e-knjige generirale tek 770 milijuna (Fruhlinger, 2018). To označava pad od 3,9% u prodaji e-knjiga (Fruhlinger, 2018). Pretpostavlja se da je to zbog toga što se ljudi žele odmaknuti od tehnologije te više čitaju fizičke kopije umjesto digitalnih (Fruhlinger, 2018). Međutim, u 2018. se uočava i jedan drugi trend, a to je rast piratstva (Kozlowski, 2018). Prema Good e-Readerovom istraživanju iz 2018. (citirano iz Kozlowski, 2018) piratstvo se povećalo za čak 12% u odnosu na godinu prije. Nadalje, nizozemska tvrtka GfK (citirano iz Kozlowski, 2018) otkriva kako je u Njemačkoj tek 10% svih e-knjiga na uređajima kupljeno. Izgleda kako DRM gubi i ovaj rat iako još uvijek ne pokazuje znakove posustajanja kao što je bio slučaj s glazbom.

5.4.1. Oblici zaštite e-knjiga

DRM tehnologije za zaštitu e-knjiga se razlikuju ovisno o vrsti uređaja i formatu e-knjige koje štite. Većina platformi koje prodaju knjige proizvode i svoje uređaje. Iz tog razloga su razvile svoje DRM tehnologije koje će uz zaštitu sadržaja osiguravati da se e-knjige

kupljene preko njihove platforme mogu koristiti samo na njihovim uređajima (kotobee.com, 2017). Trenutno najpopularnije tehnologije su Adobe ADEPT, FairPlay i Amazon DRM.

5.4.1.1. Adobe ADEPT

ADEPT je rješenje koje je razvio Adobe, a primjenjuje se na EPUB i PDF formatima e-knjiga. Za razliku od FairPlaya i Amazon DRM-a, ova tehnologija se ne ograničava na uređaje samo jednog proizvođača (kotobee.com, 2017). E-knjige zaštićene ADEPTOM mogu se čitati na mnogim Android uređajima, računalima te na svim čitačima e-knjiga osim Kindlea (kotobee.com, 2017). Međutim, jedan korisnik može čitati e-knjigu na samo 6 uređaja (Hoepman, 2012). Također, korisnik mora instalirati Adobe Digital Editions (ADE) jer jedino taj softver može čitati sadržaj zaštićen ADEPT-om. U ADEPT sustavu obično sudjeluju tri entiteta, a to su:

1. Korisnik koji pokreće Adobe Digital Editions;
2. Distributer koji pokreće Adobe Content Server;
3. Adobe (Hoepman, 2012).

ADEPT funkcionira na sljedeći način. Svaka digitalna kopija iste knjige se kriptira istim ključem koji se zove knjiški ključ (eng. book key) (Hoepman, 2012). Biranje tog ključa te sam postupak kriptiranja e-knjiga obavlja distributer (Hoepman, 2012). Uz taj knjiški ključ postoji i korisnički ključ (eng. user key) koji se generira instalacijom ADE-a i koji se zatim šalje u Adobe (Hoepman, 2012). Sa svojim Adobe ID-om, korisnik može aktivirati do 6 uređaja od kojih će svaki koristiti korisnički ključ jedinstven za taj uređaj (Hoepman, 2012). Budući da se licence izdaju ključevima, samo uređaji s tim ključem će moći čitati e-knjigu (Hoepman, 2012). Licencu dobavlja ADE kada korisnik kupi e-knjigu (Hoepman, 2012).

5.4.1.2. Amazon DRM

Amazon DRM je Amazonova tehnologija za zaštitu knjiga koje oni distribuiraju. Dakle, to se odnosi samo na njihove AZW i KF8 formate e-knjiga (Lister, n.d.). Za razliku od ADEPT-a, e-knjige zaštićene ovom tehnologijom se ne mogu čitati ni na jednom drugom uređaju osim Kindlea (kotobee.com, 2017). Amazon na taj način osigurava da samo kupac ima pristup njihovom sadržaju (kotobee.com, 2017). Sve ostale karakteristike su više manje slične ADEPT-u poput ograničenog broja uređaja koji se mogu aktivirati na jednom računu te razni mehanizmi kod kriptiranja i dekriptiranja e-knjige (Lister, n.d.). Naravno, na izdavačima je da

odluče hoće li staviti DRM na e-knjige ili ne. Sama Amazon platforma ne daje jasne informacije o DRM zaštiti na knjigama pa se eventualna odsutnost DRM-a može vidjeti tek nakon kupnje (Lister n.d.).

Iako su formati AZW i KF8 namijenjeni isključivo za Kindle, na njega se mogu prenijeti e-knjige drugih formata koje nemaju DRM zaštitu (Lister, n.d.). Ipak, takve e-knjige neće biti dio online zbirke što znači da se neće moći povrnuti ukoliko se Kindle uređaj izgubi ili zamijeni (Lister, n.d.).

5.4.1.3. FairPlay

FairPlay je već bio spomenut kao jedna od tehnologija koja se koristila za zaštitu glazbe kupljene na iTunes platformi. U 2009. se ova tehnologija prestala primjenjivati na glazbu, ali ne i na ostale digitalne sadržaje. Ova tehnologija je zapravo Appleova verzija Amazonovog DRM-a, međutim, formati e-knjiga koji se štite FairPlayom su drugačiji. EPUB i noviji Appleov format IBA su formati u kojima se prodaju knjige preko Apple Booksa pa su iz tog razloga oni jedini zaštićeni FairPlayom (Lister, 2018). Ograničenja korištenja su gotovo jednaka Amazonovom DRM-u pa se tako e-knjige mogu čitati samo na Appleovim uređajima (Lister, 2018). Isto tako, sadržaj se može pregledavati na samo 5 autoriziranih Appleovih uređaja (Gaber, 2013).

FairPlay funkcionira na sljedeći način. Kod kupnje sadržaja, iTunes ili, u ovom slučaju, Apple Books šalje kupcu korisnički ključ, glavni ključ koji je kriptriran korisničkim te sadržaj kriptiran glavnim ključem (Gaber, 2013). Kod aktivacije Apple uređaja, Apple Books na temelju jedinstvenih karakteristika uređaja poput imena CPU-a kreira jedinstveni identifikator (Gaber, 2013). Taj jedinstveni identifikator služi kao korisnički ključ za određeni uređaj (Gaber, 2013). Naposljetku, kada korisnik otvara kupljenu e-knjigu, Apple Books aplikacija obavlja sljedeće radnje:

1. Koristi korisnički ključ da dekriptira glavni ključ;
2. Koristi glavni ključ da dekriptira sadržaj;
3. Pregledava sadržaj prema pravima korištenja (Gaber, 2013).

6. Zaključak

Tehnologije za upravljanje digitalnim pravima su razne i nude zaštitu za gotovo svaku vrstu digitalnog sadržaja. Međutim, njihova zaštita digitalnog sadržaja uglavnom uključuje brojna ograničenja za korisnike, a nerijetko i narušavanje kvalitete i uporabljivosti sadržaja. U videoigrama je njihova prisutnost najočitija jer o njima ovisi hoće li se igra uopće moći pokrenuti i koliko će se njene performanse smanjiti. Filmovi i e-knjige s druge strane imaju blaža ograničenja. Tako se kod filmova na streaming platformama jedino sprječava snimanje sadržaja dok se e-knjige mogu čitati na određenom broju uređaja što se i ne primjećuje u tolikoj mjeri. Ipak kod e-knjiga je problem što distributeri poput Applea i Amazona svojim DRM tehnologijama ne dozvoljavaju korištenje sadržaja kupljenih preko njihovih platformi na uređajima koji nisu njihovi. Stoga je jasno da DRM tehnologije poboljšavaju zaštitu sadržaja na račun uporabljivosti istog. Međutim, problem je taj što se gotovo svaka zaštita može probiti. U Denuvu to znaju pa im je sa svakom novom igrom cilj odgoditi njihovu piratizaciju na što je dulje moguće, ali u zadnje vrijeme ni u tome ne uspijevaju. Slična je stvar i s tvrtkama koje stvaraju tehnologije za zaštitu e-knjiga čije se DRM zaštite mogu vrlo lako maknuti uz pomoć raznih alata. Jedini digitalni sadržaj kod kojeg je prepoznata uzaludnost DRM-a jest glazba. Apple je prepoznao besmisao zaštite digitalne glazbe, ali nije jasno zašto se isto nije prepoznalo kod ostalih digitalnih sadržaja.

Izgleda kako će se DRM tehnologije nastaviti razvijati u budućnosti s upitnom uspješnošću zaštite sadržaja i još upitnijim utjecajem na samu kvalitetu sadržaja. Budući da pirati također nemaju namjeru stati s probijanjem tih zaštita i neovlaštenom distribucijom digitalnih sadržaja, pred korisnikom će stajati izbor – kupovati DRM sadržaj ili ilegalno dobavljati isti. No, sve dok će postojati autori i izdavači koji će odbijati stavljati DRM zaštitu na svoja djela, budućnost neće biti toliko crna.

7. Literatura

Alexander, L. (2009). Valve Unveils New Anti-Piracy, In-Game DLC Features To Steamworks. [online] Gamasutra.com. Dostupno na: https://www.gamasutra.com/view/news/113829/Valve_Unveils_New_AntiPiracy_InGame_DLC_Features_To_Steamworks.php [Pristupljeno 1. 7. 2019].

Bott, E. (2010). iTunes alternatives: how do Amazon and other digital music services compare? | ZDNet. [online] ZDNet. Dostupno na: https://www.zdnet.com/article/itunes-alternatives-how-do-amazon-and-other-digital-music-services-compare/ [Pristupljeno 1. 7. 2019].

Corson-Knowles, T. (n.d.). What is an eBook? and 8 Reasons You Should Read Them | TCK Publishing. [online] TCK Publishing. Dostupno na: https://www.tckpublishing.com/what-is-an-ebook/ [Pristupljeno 1. 7. 2019].

Demerjian, C. (2009). A closer look at Valve's CEG. [online] The Inquirer. Dostupno na: https://www.theinquirer.net/inquirer/news/1051534/a-closer-look-valve-ceg [Pristupljeno 1. 7. 2019].

Ell, K. (2018). Video game industry is booming with continued revenue. [online] CNBC. Dostupno na: https://www.cnbc.com/2018/07/18/video-game-industry-is-booming-with-continued-revenue.html [Pristupljeno 1. 7. 2019].

Fenlon, W. (2019). Denuvo DRM cracks seem to be happening faster and faster. [online] pcgamer. Dostupno na: https://www.pcgamer.com/denuvo-cracks-2019/ [Pristupljeno 1. 7. 2019].

Fruhlinger, J. (2018). Are E-Books Finally Over? The Publishing Industry Unexpectedly Tilts Back to Print. [online] Observer. Dostupno na: https://observer.com/2018/11/ebook-sales-decline-independent-bookstores/ [Pristupljeno 1. 7. 2019].

Gaber, Tarek. (2013). Digital Rights Management: Open Issues to Support e-Commerce. U H. El-Gohary i R. Eid (ur.), *E-Marketing in Developed and Developing Countries: Emerging Practices* (str. 69-87). Hershey: IGI Global

Godwin, M. (2004) What Every Citizen Should Know About DRM, a.k.a. “Digital Rights Management”. [pdf] Digital Rights Management, PublicKnowledge. Dostupno na: http://www.publicknowledge.org/pdf/citizens_guide_to_drm.pdf [Pristupljeno 1. 7. 2019].

Grubb, J. (2015). Dota 2 makes $18M per month for Valve — but League of Legends makes that much every 5 days. [online] VentureBeat. Dostupno na: https://venturebeat.com/2015/03/24/dota-2-makes-18m-per-month-for-valve-but-league-of-legends-makes-that-much-every-5-days/ [Pristupljeno 1. 7. 2019].

Guevin, J. (2009). EA hit with class action suit over 'Spore'. [online] CNET. Dostupno na: https://www.cnet.com/news/ea-hit-with-class-action-suit-over-spore/ [Pristupljeno 1. 7. 2019].

Hachman, M. (2017). Tested: Microsoft Edge is the only browser to run Netflix in 4K. [online] PCWorld. Dostupno na: https://www.pcworld.com/article/3181818/tested-microsoft-edge-is-the-only-browser-to-run-netflix-in-4k.html [Pristupljeno 1. 7. 2019].

Harris, M. (2019). Apple's FairPlay Copy Protection: How Does it Work?. [online] Lifewire. Dostupno na: https://www.lifewire.com/what-is-apple-fairplay-drm-2438229 [Pristupljeno 1. 7. 2019].

Harris, M. (2019). The History of Napster: Yes, It's Still Around. [online] Lifewire. Dostupno na: https://www.lifewire.com/history-of-napster-2438592 [Pristupljeno 1. 7. 2019].

Hoepman, J. (2012). Analysing ADEPT (Adobe Digital Experience Protection Technology). [online] Blog.xot.nl. Dostupno na: https://blog.xot.nl/2012/04/12/analysing-adept-adobe-digital-experience-protection-technology/ [Pristupljeno 1. 7. 2019].

Hoffman, C. (2018). What Is Denuvo, and Why Do Gamers Hate It?. [online] How-To Geek. Dostupno na: https://www.howtogeek.com/400126/what-is-denuvo-and-why-do-gamers-hate-it/ [Pristupljeno 1. 7. 2019].

Iannella, R. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine. Dostupno na: http://www.dlib.org/dlib/june01/iannella/06iannella.html

Ibisworld.com. (2018). IBISWorld - Industry Market Research, Reports, and Statistics. [online] Dostupno na: https://www.ibisworld.com/industry-trends/global-industry-reports/other-

community-social-personal-service-activities/movie-production-distribution.html [Pristupljeno 1. 7. 2019].

Karmali, L. (2012). Ubisoft Officially Ditches Always-On PC DRM - IGN. [online] IGN. Dostupno na: https://www.ign.com/articles/2012/09/05/ubisoft-officially-ditches-always-on-pc-drm [Pristupljeno 1. 7. 2019].

Khan, I. (2019). Square Enix Added, And Is Now Removing, Always-Online DRM From Final Fantasy X On PC. [online] Game Informer. Dostupno na: https://www.gameinformer.com/2019/03/27/square-enix-added-and-is-now-removing-always-online-drm-from-final-fantasy-x-on-pc [Pristupljeno 1. 7. 2019].

Klappenbach, M. (2017). What are the Best Digital Download Platforms for PC Games?. [online] Lifewire. Dostupno na: https://www.lifewire.com/top-pc-game-digital-download-services-813065 [Pristupljeno 1. 7. 2019].

Kozlowski, M. (2018). eBook Piracy is on the rise in 2018. [online] Good e-Reader. Dostupno na: https://goodereader.com/blog/e-book-news/ebook-piracy-is-on-the-rise-in-2018 [Pristupljeno 1. 7. 2019].

Lamont, T. (2013). Napster: the day the music was set free. [online] the Guardian. Dostupno na: https://www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing [Pristupljeno 1. 7. 2019].

Layton, J. (2006). How Digital Rights Management Works. [online] HowStuffWorks. Dostupno na: https://computer.howstuffworks.com/drm.htm [Pristupljeno 1. 7. 2019].

Lister, J. (2018). How to Read iBooks on Windows. [online] Techwalla. Dostupno na: https://www.techwalla.com/articles/how-to-read-ibooks-on-windows [Pristupljeno 1. 7. 2019].

Lister, J. (n.d.). What Is Kindle DRM?. [online] Itstillworks.com. Dostupno na: https://itstillworks.com/kindle-drm-17841.html [Pristupljeno 1. 7. 2019].

MacDailyNews. (2007). Apple CEO Steve Jobs' posts rare open letter: 'Thoughts on Music' – calls for DRM-free music. [online] Dostupno na:

https://macdailynews.com/2007/02/06/apple_ceo_steve_jobs_posts_rare_open_letter_thoughts_on_music/ [Pristupljeno 1. 7. 2019].

Makuch, E. (2018). Dota 2 The International Tournament Prize Pool Sets A New Record. [online] Gamespot. Dostupno na: https://www.gamespot.com/articles/dota-2-the-international-tournament-prize-pool-set/1100-6461253/ [Pristupljeno 1. 7. 2019].

Mendez, J. (2017). How Steam Employs DRM & What That Means For Your Game. [online] Black Shell Media. Dostupno na: https://blackshellmedia.com/2017/06/28/steam-employs-drm-means-game/ [Pristupljeno 1. 7. 2019].

Morrison, G. (2014). HDCP 2.2: What you need to know. [online] CNET. Dostupno na: https://www.cnet.com/news/hdcp-2-2-what-you-need-to-know/ [Pristupljeno 1. 7. 2019].

OMA. (2011). OMA Digital Rights Management V2.0.1, Open Mobile Alliance Ltd. Dostupno na: http://www.openmobilealliance.org/release/DRM/V2_0_2-20080723-A/OMA-AD-DRM-V2_0_1-20080226-A.pdf

Palumbo, A. (2018). Tekken 7 Director Says Denuvo DRM Is Causing Performance Issues In The Game. [online] Wccftech. Dostupno na: https://wccftech.com/tekken-7-denuvo-drm-performance-issues/ [Pristupljeno 1. 7. 2019].

Papadopoulos, J. (2018). Bethesda and Arkane Studios have removed the Denuvo anti-tamper tech from Dishonored 2 | DSOGaming | The Dark Side Of Gaming. [online] Dsogaming.com. Dostupno na: https://www.dsogaming.com/news/bethesda-and-arkane-studios-have-removed-the-denuvo-anti-tamper-tech-from-dishonored-2/ [Pristupljeno 1. 7. 2019].

Purchese, R. (2014). Don't call it DRM: what's Denuvo Anti-Tamper?. [online] Eurogamer.net. Dostupno na: https://www.eurogamer.net/articles/2014-12-19-denuvo-anti-tamper-drm [Pristupljeno 1. 7. 2019].

Richard, M. (2016). Darkspore Servers Shut Down. [online] Gaming News, Reviews, and Articles - TechRaptor.net. Dostupno na: https://techraptor.net/content/ea-shuts-down-darkspore-servers [Pristupljeno 1. 7. 2019].

Sicker, D., Ohm, P. and Gunaji, S. (2007). The Analog Hole and the Price of Music: an Empirical Study. U M. Schwalb (ur.), *Journal on Telecommunications and High Technology Law, Vol. 5, 2007*. Boulder: Journal on Telecommunications & High Technology Law

Smith, E. (2017). The Incredibly Technical History of Digital Rights Management. [online] Vice. Dostupno na: https://www.vice.com/en_us/article/evbgkn/the-incredibly-technical-history-of-digital-rights-management [Pristupljeno 1. 7. 2019].

Taylor, H. (2018). Irdeto acquires Denuvo in bid to beef up security for the games industry. [online] GamesIndustry.biz. Dostupno na: https://www.gamesindustry.biz/articles/2018-01-23-irdeto-acquires-denuvo-in-bid-to-beef-up-security-in-the-games-industry [Pristupljeno 1. 7. 2019].

Triggs, R. (2019). Widevine digital rights management explained. [online] Android Authority. Dostupno na: https://www.androidauthority.com/widevine-explained-821935/ [Pristupljeno 1. 7. 2019].

VdoCipher Blog. (n.d.). Microsoft Playready DRM: Infrastructure Implementation for Premium Content - VdoCipher Blog. [online] Dostupno na: https://www.vdocipher.com/blog/microsoft-playready-drm-infrastructure-implementation-for-premium-content/ [Pristupljeno 1. 7. 2019].

VdoCipher Blog. (n.d.). Widevine DRM & CDM for Security of Premium Content - VdoCipher Blog. [online] Dostupno na: https://www.vdocipher.com/blog/widevine-drm-hollywood-video/ [Pristupljeno 1. 7. 2019].

VIXY Video Platform. (2017). Why DRM? 5 things you always wondered about Digital Rights Management - VIXY Video Platform. [online] Dostupno na: https://www.vixyvideo.com/5-things-you-always-wondered-about-digital-rights-management/ [Pristupljeno 1. 7. 2019].

Upravljanje digitalnim pravima na Internetu

Sažetak

Zbog sve veće dostupnosti informacija i digitalnih sadržaja, autorima i izdavačima je teže zaštititi svoje vlasništvo. Iz tog razloga se poseže za raznim oblicima zaštite sadržaja koji se skupa nazivaju upravljanje digitalnim pravima (eng. Digital Rights Management - DRM). Cilj i svrha ovog rada je pobliže objasniti upravljanje digitalnim pravima, tehnologije koje se koriste te načine na koje se one primjenjuju na digitalne sadržaje poput filmova, glazbe, videoigara i e-knjiga. Također, u radu će se ukazati i na loše strane DRM-a. Prvenstveno se pod time misli na ograničavanje uporabe sadržaja što se u nekim slučajevima izuzetno negativno odražava na same kupce.

Ključne riječi: DRM, licenca, Denuvo, Widevine, FairPlay, Netflix

Digital Rights Management on the Internet

Summary

Due to the increasing availability of information and digital content, it is more difficult for authors and publishers to protect their works. Because of this, they are reaching out for various forms of content protection, commonly referred to as Digital Rights Management (DRM). The purpose of this paper is to explain the digital rights management, the technologies used and the ways in which they are applied to digital content such as movies, music, video games and e-books. Also, the paper will point out the obstructive aspects of DRM such as restrictions on the usage of digital content which negatively reflect on the consumers.

Key words: DRM, licence, Denuvo, Widevine, FairPlay, Netflix