HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje digitalnim pravima (DRM)

CCERT-PUBDOC-2007-10-207

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Upravljanje digitalnim pravima (eng. *Digital Rights Managemet - DRM*) zajednički je naziv skupa tehnologija za kontrolu pristupa koje izdavači i drugi vlasnici autorskih prava koriste za ograničavanje pristupa digitalnim uređajima i multimedijalnim sadržajima. Ovaj pojam ima dodirnih točaka sa zaštitom od kopiranja (eng. *copy protection*), ali DRM sustavi se prije svega koriste za zaštitu kreativnih sadržaja, kao što su glazba i film, dok se zaštita od kopiranja najčešće odnosi na programsku podršku (eng. *software*).

Korištenje sustava za upravljanje digitalnim pravima, od samih njihovih početaka, izvor je brojnih kontroverzi. Pobornici DRM tehnologija tvrde kako su one vlasnicima autorskih prava nužne za onemogućavanje neovlaštenog kopiranja, a samim time i osiguravanje konstantnog priljeva prihoda. Kritičari, kao što je FSF (eng. *Free Software Foundation*) neprofitna korporacija, ustraju na stavu da se ne radi o upravljanju pravima već isključivo o nametanju ograničenja pa akronim DRM duhovito interpretiraju kao *Digital Restriction Management*. Njihov stav je da vlasnici autorskih prava DRM tehnologijama pokušavaju nametnuti ograničenja koja nadilaze zakonske okvire. EFF (eng. *Electronic Frontier Foundation*) organizacija, drugi veliki protivnik sustava za upravljanje digitalnim pravima, ove tehnologije smatra načinom ograničavanja tržišne utakmice onemogućavanjem konkurencije.

U nastavku dokumenta slijedi detaljnije definiranje DRM tehnologija uz povijesni osvrt, prikaz najčešće korištenih tehnologija za zaštitu video i audio sadržaja te dokumenata, kratak pregled pravnih aspekata implementacije ovih tehnologija te opis njihovih najznačajnijih nedostataka.

2. Općenito o DRM-u

Namjena DRM tehnologija je kontrola korištenja digitalnih sadržaja putem onemogućavanja pristupa, kopiranja i pretvorbe u druge formate. Kroz povijest, vlasnici autorskih prava, sami autori te druge financijski ili umjetnički zainteresirane strane protivile su se tehnologijama koje omogućuju kopiranje sadržaja. Primjeri upravljanjima pravima, prije dolaska digitalnih tehnologija, obuhvaćaju zaštitu perforiranih traka namijenjenih mehaničkim glasovirima s početka 20. stoljeća te zaštitu audio i video magnetskih vrpci.

Digitalni formati zapisa sadržaja značajno olakšavaju kopiranje sadržaja zbog čega su umnogostručeni napori vlasnika autorskih prava uloženi u njihovu zaštitu. Uzastopnim kopiranjem sadržaja s analognih medija neizbježno se gubi kvaliteta dok se digitalni mediji, ponekad čak i tijekom normalne uporabe, mogu kopirati neograničen broj puta bez ikakvog gubitka kvalitete. Popularizacija osobnih računala, lakoća snimanja sadržaja audio CD medija (eng. *CD ripping*) i radio emisija, uz popularne servise za razmjenu datoteka na Internetu, učinili su razmjenu neautoriziranih kopija zaštićenih sadržaja (eng. *digital piracy*) iznimno jednostavnom.

Iako je kontrola reprodukcije i korištenja programske podrške s prekidima u uporabi od 1970-ih godina, naziv DRM odnosi se prije svega na autorske sadržaje, kao što su na primjer umjetnička djela. Pojedini kritičari DRM tehnologija ističu kako, pored sprječavanja zlouporabe zaštićenih sadržaja, upravljanje digitalnim pravima ponekad onemogućuje i njihovu legalnu upotrebu.

Upravljanje digitalnim pravima nad sadržajima najviše se koristi u zabavnoj industriji, npr. u filmskoj i glazbenoj industriji, ali se pojavljuje i na drugim područjima. Mnoge tvrtke koje se bave prodajom glazbe na Internetu, kao što je *iTunes*, te pojedini izdavači elektroničkih knjiga (eng. *e-books*) razvile su različite strategija upravljanja digitalnim pravima. Tijekom posljednjih godina brojni televizijski producenti zahtijevaju implementaciju DRM mjera kako bi se kontrolirao pristup njihovim programima zbog rasta popularnosti DRV (eng. *Digital Video Recorder*) uređaja.

3. Prikaz najčešće korištenih tehnologija

Tehnologije upravljanja digitalnim pravima moguće je, prema području primjene, podijeliti na tehnologije korištene za zaštitu video sadržaja, odnosno filmova, audio sadržaja, odnosno glazbe, i tehnologije za zaštitu dokumenata.

3.1. Film

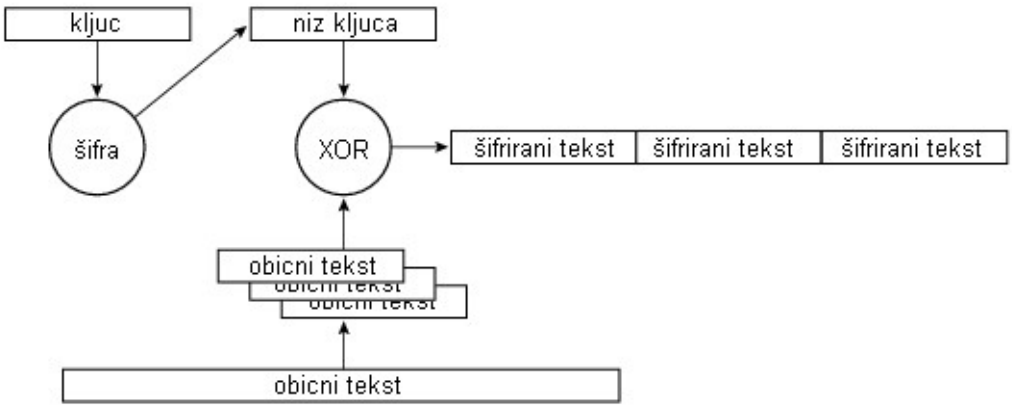
Za upravljanje digitalnim pravima pri rukovanju video sadržajima najčešće se koriste, sada već zastario, CSS sustav, noviji PMP sustav integriran u *Vista* operacijski sustav te AACS standard.

3.1.1. CSS

CSS (eng. *Content Scramble System*) je DRM sustav korišten kod gotovo svih komercijalnih DVD-Video diskova, a uveden je 1996. godine. Za zaštitu sadržaja koristi zaštićenu 40-bitnu enkripciju niza (eng. *stream cipher*). Kod enkripcije niza pojedini znakovi zaštićenog sadržaja kombiniraju se s pseudonasumičnim ključem (eng. *keystream*), najčešće XOR (eng. *eXclusive OR*) operacijom. Ilustracija enkripcije niza dana je slikom *Slika 1*.

Skupovi CSS ključeva licencirani su pojedinim proizvođačima koji ih ugrađuju u svoje DVD čitače i diskove. Većina DVD čitača opremljena je modulom za dekripciju CSS sadržaja. CSS ključ zajednički je naziv za autorizacijski ključ, ključ diska, ključ čitača, ključ filma, skup ključeva drugog diska i/ili enkripcijski ključ.

U lipnju 1999. godine Jon Lech Johansen i još dvije osobe, čiji identitet nije poznat, probili su CSS algoritam te izdali DeCCS alat za dekripciju. Ubrzo nakon toga pokazano je kako je CSS algoritam izrazito ranjiv na napade pokušajima i pogreškama (eng. *brute force attack*). Slabost ovog algoritma rezultat je zakonskih ograničenja izvoza kriptografskih tehnologija koja postoje u Sjedinjenim Državama. Kod novijih sustava za reprodukciju video sadržaja CSS zaštita zamijenjena je naprednijim DRM sustavima.



Slika 1: Primjer enkripcije niza

3.1.2. PMP

PMP (eng. *Protected Media Path*) skup je tehnologija za stvaranje „zaštićenog okruženja" (eng. *Protected Environment*), a prvi puta je implementiran kod *Microsoft Windows Vista* operacijskog sustava. Podskupovi PMP sustava su PVP (eng. *Protected Video Path*) i PUMA (eng. *Protected User Mode Audio*) tehnologije.

Zaštićeno područje, unutar kojega se reproducira DRM sadržaj, sadrži medijske komponente zadužene za reprodukciju. Pojedina aplikacija zaštićenom području prosljeđuje udaljene kontrole (reproduciraj, pauziraj, premotaj isl.) bez potrebe za rukovanjem nezaštićenim podacima. Ovo područje također sadrži podršku za odobrene programske module drugih proizvođača.

Kako bi se spriječilo neovlašteno kopiranje DRM sadržaja, *Vista* operacijski sustav provodi njihovu izolaciju te kontinuirani nadzor nad aktivnim programskim modulima na razini jezgre. U slučaju uočavanja aktivnosti neovjerene programske komponente, obustavlja se reprodukcija DRM sadržaja. Zaštićeno okruženje u potpunosti je programski implementirano pa postoji mogućnost ranjivosti na napade na programskoj razini, primjerice izmjenama jezgre *Vista* operacijskog sustava.

Ograničenja koja nameće PMP sustav odnose se na različite izlaze iz osobnog računala. Tako digitalni izlazi, kao što su DVI (eng. *Digital Visual Interface*) i HDMI (eng. *High-Definition Multimedia Interface*), moraju imati uključenu HDCP (eng. *High-band Digital Content Protection*) zaštitu koja onemogućuje snimanje digitalnog toka podataka. Čak i analogni izlazi, namijenjeni spajanju na televizor, zahtijevaju određena ograničenja omogućena mehanizmima kao što su *Microvision* i CGMS-A (eng. *Copy Generation Management System - Analog*).

Kod *Vista* operacijskog sustava robusna kontrola video izlaza osobnog računala implementirana je PVP-OPM (eng. *Protected Video Path - Outpu Protection Management*) protokolom koji predstavlja novu generaciju COPP (eng. *Certified Output Protection Protocol*) protokola korištenog kod *Windows XP* operacijskog sustava. Za razliku od COPP protokola, PVP-OPM nije programsko API (eng. *Application Programing Interface*) sučelje već ovaj protokol rukuje izravno medijskim komponentama unutar zaštićenog okruženja.

PVP-UAB (eng. *PVP - User-Accessible Bus*) protokol kriptira video i audio sadržaje koji se prenose *PCI-Express* sabirnicom kako bi se onemogućilo njihovo presretanje i kopiranje na putu prema grafičkoj kartici. Ovaj protokol predstavlja nadopunu PVP-OPM protokolu.

PMP ograničenja odnose se na DRM sadržaje, kao što su HD DVD ili kriptirani *Blu-ray* diskovi, čije manipuliranje je ograničeno i kod *Windows XP* operacijskog sustava, u slučaju korištenja ovlaštenih aplikacija za reprodukciju. Ograničenja se ne odnose na sadržaje bez DRM zaštite.

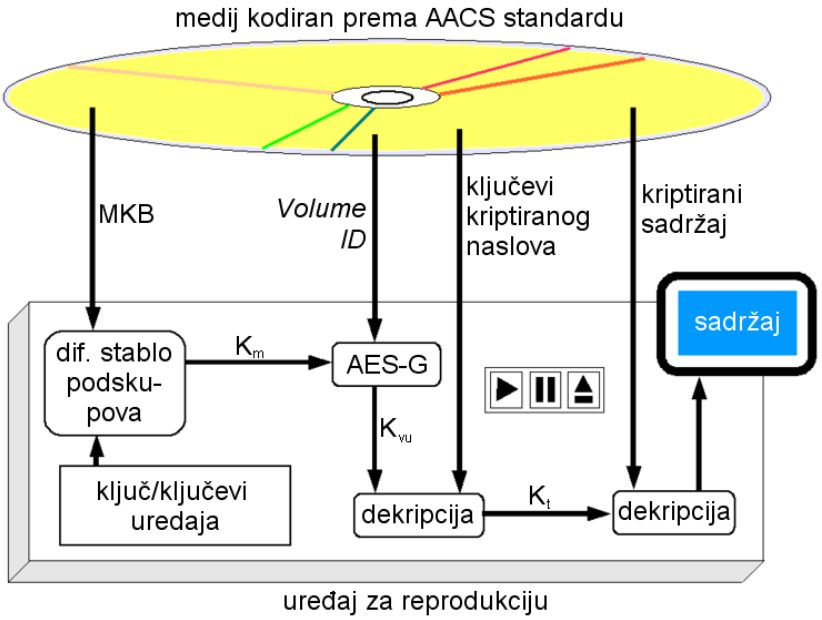
3.1.3. AACS

AACS (eng. *Advanced Access Content System*) je standard za distribuciju sadržaja i upravljanje pravima njihova korištenja namijenjen ograničavanju pristupa i onemogućavanju kopiranja sadržaja pohranjenih na optičkim diskovima nove generacije. Specifikacija standarda objavljena je u travnju 2005. godine i prihvaćena od strane proizvođača kao osnova zaštite HD DVD i *Blu-ray* diskova.

Standard je razvijen od strane AACS LA (eng. *AACS Licensing Administrator*) konzorcija koji se sastoji od tvrtki: *Disney*, *Intel*, *Microsoft*, *Panasonic*, *Warner Brothers*, IBM, *Toshiba* i *Sony*.
AACS zaštita sadržaja temelji se na njegovom kriptiranju. Enkripcija se provodi pomoću jednog ili više ključeva naslova (eng. *title key*) prema AES (eng. *Advanced Encryption Standard*) standardu. Ključevi naslova stvaraju se na temelju kombinacije medijskog ključa (eng. *media key*) i nekoliko drugih elemenata, koji uključuju *Volume ID* identifikacijsku oznaku medija (npr. serijski broj fizički upisan na DVD disku) i vrijednosti dobivene izvođenjem jednosmjerne funkcije (eng. *cryptographic hash*) nad pravilima korištenja danog sadržaja.
Osnovna razlika između AACS i CSS sustava leži u organizaciji dekripcijskih ključeva unutar uređaja za reprodukciju. Kod CSS sustava svi uređaji istog modela imaju jednak dekripcijski ključ. Sadržaji su kriptirani prema ključu ovisnom o naslovu, a taj je ključ zatim kriptiran pomoću ključa vezanog uz model uređaja. Zbog toga svaki disk sadrži nekoliko stotina enkripcijskih ključeva, po jedan za svaki licencirani model uređaja za reprodukciju. Takav pristup omogućuje opoziv određenog modela uređaja za reprodukciju izuzimanjem njegova dekripcijskog ključa s budućih izdanja. Dodatni nedostatak CCS DRM sustava je povećana ranjivost zbog jednakog ključa pohranjenog u velikom broju uređaja, što jasno pokazuju brojni slučajevi probijanja zaštite iz sredine 90-ih godina prošlog stoljeća.
Prema AACS standardu svaki uređaj opremljen je jedinstvenim skupom dekripcijskih ključeva koji se koriste u sustavu kriptiranja emisija (eng. *broadcast encription*). Ovaj pristup vlasniku licence omogućuje opozivanje pojedinog uređaja za reprodukciju, odnosno njegova skupa dekripcijskih ključeva. Ako zlonamjeran korisnik probije zaštitu određenog uređaja i objavi njegove ključeve, organizacija za upravljanje AACS licencama može jednostavno onemogućiti reprodukciju budućih naslova na spomenutom uređaju.
Čak i ako napadač pokuša kompromitirani skup ključeva sačuvati tajnim, objavljujući samo dekriptirane sadržaje, unutar AACS standarda postoji mehanizam otkrivanja o kojim ključevima, odnosno uređaju, se radi. AACS standard omogućuje dekripciju različitih inačica kratkih dijelova filma pomoću različitih ključeva. Pojedini uređaj može dekriptirati samo po jednu inačicu svakog od tih dijelova. Umetanjem digitalnih žigova u različite dijelove filma i analizom koji se od žigova pojavljuju u piratiziranoj inačici moguće je utvrditi kompromitirane ključeve i opozvati ih.
AACS sustavi za upravljanje digitalnim pravima temelje se na jedinstvenim *Volume ID* identifikacijskim oznakama zapisanim na medije pomoću posebnih uređaja. Ove oznake nemoguće je kopirati na medije koje korisnici mogu snimati. Time je onemogućeno jednostavno bit-po-bit kopiranje medija, jer je za reprodukciju zaštićenog sadržaja nužna, ali ne i dovoljna, *Volume ID* oznaka. Za čitanje spomenute oznake potreban je kriptografski certifikat (eng. *Private Host Key*) potpisan od strane AACS LA tijela, iako postoje tvrdnje o mogućnosti zaobilaženja ove zaštite izmjenama ugrađene programske podrške (eng. *firmware*) uređaja za reprodukciju.
Disk sa sadržajem zaštićenim prema AACS standardu sadrži:

- MKB (eng. *Media Key Block*) blok,
- *Volume ID* identifikacijsku oznaku,
- ključeve kriptiranog naslova (eng. *Encrypted Title Keys*) i
- kriptirani sadržaj (eng. *Encrypted Content*).

MKB blok je kriptiran u diferencijalnom stablu podskupova (eng. *subset difference tree*), što znači da je pomoću svakog ključa moguće pronaći bilo koji drugi ključ stabla, osim njegova roditeljskog ključa. Zbog toga je za opozivanje uređaja dovoljno MKB kriptirati roditeljskim ključem danog uređaja.
MKB blok nakon dekriptiranja daje *Km* (eng. *Media Key*). *Km* se nakon toga kombinira s *Volume ID* oznakom u postupku jednosmjerne enkripcije (AES-G) koji rezultira *Kvu* (eng. *Volume Unique Key*) ključem. Pomoću *Kvu* ključa dekriptiraju se ključevi kriptiranog naslova (K_t) koji se potom koriste za dekripciju samog filma. Opisani postupak ilustriran je slikom *Slika 2*.



Slika 2: Postupak reprodukcije sadržaja kodiranog prema AACS standardu

3.2. Glazba

Kod tehnologija upravljanja digitalnim pravima nad audio sadržajima razlikuju se tehnologije primijenjene na audio CD medije te one namijenjene zaštiti glazbe na Internetu.

3.2.1. Audio CD mediji

Tvrtka *Bertelsmann* prva je, 2002. godine, upotrijebila DRM tehnologije za zaštitu sadržaja audio CD diskova. Isprva se zaštita primjenjivala samo na promotivnim diskovima, no s vremenom se počela ugrađivati kod svih diskova spomenute tvrtke. Nedostaci njihove DRM tehnologije uključuju:

- nemogućnost reprodukcije diskova na svim čitačima,
- nemogućnost reprodukcije diskova na osobnim računalima te
- rušenje Windows operacijskog sustava u slučaju pokušaja reprodukcije zaštićenog diska.

Sony BMG 2005. godine uvodi vlastitu DRM tehnologiju koja se sastoji od instalacije DRM aplikacije na korisnikovu računalu. Instalacija spomenute aplikacije provodi se bez jasne obavijesti korisniku i bez potrebe za njegovim pristankom. Ovaj programski paket, među ostalim, sadrži i alat koji utječe na rad operacijskog sustava (eng. *rootkit*), a koji operacijski sustav čini izrazito ranjivim na napade zlonamjernih korisnika. Nakon otkrića brojnih nedostataka DRM aplikacije Sony je pokušao umanjiti značaj propusta, ali je naposljetku bio prisiljen opozvati milione CD diskova, izdati nekoliko zakrpa namijenjenih uklanjanju ranjive aplikacije te vratiti novac korisnicima koji su pokrenuli tužbe. Pored sigurnosnih propusta DRM tehnologija tvrtke *Sony BMG* ima i značajne funkcionalne nedostatke:

- sadržaj je zaštićen samo u slučaju reprodukcije na Windows operacijskim sustavima, ne i na drugoj opremi,
- zaštita na Windows operacijskim sustavima redovno je probijana od strane zlonamjernih korisnika,
- zaštitu je moguće jednostavno zaobići držanjem *Shift* tipke rijekom umetanja diska ili onemogućavanjem automatskog pokretanja diska nakon umetanja (eng. *autorun*),
- audio zapise moguće je reproducirati i snimati čime se u potpunosti zaobilazi DRM zaštita, tzv. analogna rupa.

Godine 2007. tvrtka EMI obustavila je objavljivanje audio CD diskova s DRM zaštitom s obrazloženjem da su troškovi zaštite značajno veći od učinaka. Do tada, EMI je bio posljednji veliki izdavač koji je na svoje audio CD diskove ugrađivao DRM zaštitu.

3.2.2. Glazba na Internetu

Brojne glazbene trgovine na Internetu koriste DRM tehnologije za ograničavanje korištenja kupljene glazbe:

- *iTune Store* trgovina, u vlasništvu *Apple Inc.*, omogućuje kupovinu pojedinih pjesama, zaštićenih *FairPlay* DRM sustavom, za 0.99 dolara. Korištenjem *iTunes Plus* usluge moguće je, za dodanih 30 centi, kupiti pjesme bez zaštite.
- *Napster* Internet trgovina nudi trajnu kupovinu pjesama te pretplatu koja omogućuje skidanje i preslušavanje pjesama s DRM zaštitom. Korisnici tijekom trajanja pretplate mogu neograničeno skidati i preslušavati glazbu u WMA (eng. *Windows Media Audio*) formatu, ali nakon obustavljanja pretplate sva skinuta glazba postaje neiskoristiva. Preslušavanje glazbe na prijenosnom uređaju naplaćuje se 5 dolara mjesečno, a snimanje na CD ili korištenje nakon isteka pretplate košta 0.99 dolara po pjesmi. Pjesme kupljene u *Napster* trgovini moguće je reproducirati na svim uređajima koji nose *PlayForSure* logo tvrtke *Microsoft*.
- *Wal-Mart Music Downloads* naplaćuje skidanje pjesama s DRM zaštitom 0.88 dolara. Zanimljiva nelogičnost kod ovog DRM sustava je mogućnost preslušavanja pjesama na *SanDisk Sansa* uređaju za reprodukciju samo ako su pohranjene u unutrašnjoj memoriji uređaja, ali ne i ako se nalaze na njegovoj *Micro SD* memorijskoj kartici.

Različite usluge trenutačno nisu kompatibilne, iako one koje koriste jednak DRM sustav (npr. *Windows Media* DRM sustav) omogućuju preslušavanje pjesama na istom uređaju. Gotovo sve Internet trgovine zahtijevaju instalaciju nekog oblika klijentske aplikacije ili dodataka (eng. *plug-in*).

Iako većina Internet trgovina koristi neki od DRM sustava, postoje i iznimke kao što su *eMusic*, *Audio Lunchbox* i *Antology records*. Pojedini izdavači također započinju s objavom pjesama bez DRM zaštite na Internetu.

3.2.3. FairPlay

FairPlay je DRM tehnologija razvijena od strane *Apple Inc.* tvrtke, a temelji se na sličnoj tehnologiji tvrtke *Veridisc*. *FairPlay* je ugrađen u *QuickTime* i *iTunes* programske pakete, *iPhone* i *iPod* uređaje te se koristi kod *iTunes Store* Internet trgovine. Ova tehnologija kriptiranjem audio datoteka AAC (eng. *Advanced Audio Coding*) formata korisnicima onemogućuje njihovu reprodukciju na neovlaštenim računalima. Svaka aplikacija koja podržava *QuickTime* može, ukoliko se nalazi na ovlaštenom računalu, reproducirati datoteke s FairPlay DRM zaštitom. To su, na primjer, *RealPlayer*, *Media Center* i *Media Player Classic* programski paketi.

Datoteke zaštićene *FairPlay* tehnologijom predstavljaju MP4 (eng. *MPEG-4 Layer 14*) kontejnere koji sadrže kriptirane audio sadržaje u AAC formatu. Enkripcija se provodi *Rijndael* algoritmom u kombinaciji s MD5 (eng. *Message-Digest algorithm 5*) jednosmjernim funkcijama.

Prilikom svakog preuzimanja pjesme pomoću *iTunes* aplikacije stvara se jedinstven nasumičan korisnički ključ kojim se kriptira glavni (eng. *master*) ključ. Korisnički ključ se, zajedno s podacima o korisničkom računu, pohranjuje na poslužitelju te ga se šalje korisnikovoj *iTunes* aplikaciji. *ITunes* paket korisničke ključeve pohranjuje u vlastitu kriptiranu bazu ključeva iz koje, prilikom reprodukcije, dohvaća korisnički ključ vezan uz određenu pjesmu. Pomoću korisničkog ključa dekriptira se glavni ključ koji se zatim koristi za dekriptiranje AAC sadržaj. Sadržaj je nakon dekripcije raspoloživ za reprodukciju.

Kada korisnik ovlasti novo računalo, *iTunes* aplikacija šalje jedinstvenu identifikacijsku oznaku tog računala poslužitelju i kao odgovor prima sve korisničke ključeve vezane uz korisnički račun. Na ovaj način tvrtka *Apple* može ograničiti broj autoriziranih računala i osigurati da svako ovlašteno računalo posjeduje sve potrebne korisničke ključeve. Ovaj postupak prikazan je slikom *Slika 3*. Kada korisnik ukloni autorizaciju određenog računala *iTunes* o tome obavješćuje poslužitelja koji uklanja identifikacijsku oznaku tog računala iz baze.

Slika 3: Raspodjela *FairPlay* korisničkih ključeva na više ovlaštenih računala

IPod uređaj također posjeduje kriptiranu bazu korisničkih ključeva. Prilikom svakog kopiranja datoteke zaštićene *FairPlay* sustavom za upravljanje digitalnim pravima na uređaj se kopira i pripadni korisnički ključ.
FairPlay ne ograničuje kopiranje datoteka, već samo omogućuje/onemogućuje njihovo dekodiranje. Prijenosni uređaji koji mogu reproducirati glazbu zaštićenu ovim DRM sustavom su: *Apple iPod*, *Motorola ROKR E1*, *Motorola SLVR* i *iPhone*.

3.3. Dokumenti

DRM tehnologije za zaštitu dokumenata usmjerene su prije svega na korporativna okruženja s ciljem onemogućavanja njihova neovlaštena korištenja (npr. industrijska špijunaža i nehotično otkrivanje). Organizacije kao što je nacionalna biblioteka *British Library* DRM sustave koriste za sigurno dostavljanje elektroničkih inačica rijetkih dokumenata, kojima su prije uvođenja takvih sustava pristup, iz pravnih razloga, imali samo ovlašteni pojedinci.
Ovu skupinu tehnologija moguće je podijeliti na E-DRM tehnologije i vodene žigove.

3.3.1. E-DRM

E-DRM (eng. *Enterprise DRM*) je zajednički naziv za sve tehnologije upravljanja digitalnim pravima korištenim za zaštitu poslovnih dokumenata u različitim formatima, kao što su *Microsoft Word*, PDF (eng. Portable Document Format), *AutoCAD* te elektronička pisma i web stranice unutar interne računalne mreže (eng. *intranet*) neke organizacije. Vlastite DRM tehnologije za zaštitu dokumenata posjeduju tvrtke: *Microsoft*, *Adobe Systems*, *Liquid Machines*, *Oracle*, *EMC Corporation* i druge.

3.3.2. Digitalni vodeni žig

Digitalni vodeni žig (eng. *watermark*) je neupadljivi element koji je u elektronički sadržaj ugrađen tijekom njegove proizvodnje ili distribucije. Moguće su različit primjene ove tehnologije, među ostalim za:

- označavanje vlasnika autorskih prava,
- označavanje distributera,
- označavanje distributivnog lanca te
- identificiranje kupca.

Digitalni žigovi nisu potpuni DRM sustavi. Oni ne štite sadržaje izravno, već se koriste kao element takvih sustava prilikom prikupljanja dokaza u sudskim procesima vezanim uz upravljanje digitalnim

pravima. Na primjer, digitalnim vodenim žigovima označene su *iTunes* pjesme čije kopiranje nije onemogućeno.

4. Zakonodavstvo i DRM

Godine 1996. zemlje članice WIPO (eng. *World Intellectual Property Organization*) međunarodne organizacije za zaštitu intelektualnog vlasništva potpisale su WCT (eng. *WIPO Copyright Treaty*) sporazum. Jedanaesti članak ovog sporazuma zemlje potpisnice obvezuje na donošenje zakona protiv izbjegavanja DRM zaštite.

Do danas, WCT sporazum implementiran je u većini članica WIPO organizacije. Američka implementacija naziva se DMCA (eng. *Digital Millennium Copyright Law*), dok je u Europi 2001. godine donesena EUCD (eng. *EU Copyright Directive*) europska direktiva o zaštiti autorskih prava koja članice Europske Unije obvezuje na donošenje potrebnih zakona. Godine 2006. donji dom francuskog parlamenta izglasao je skupinu takvih zakona pod nazivom DADVSI (fra. *Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information*). Ono što francuske zakone razlikuje od sličnih zakona drugih zemalja zahtjev je za međusobnom kompatibilnošću DRM sustava.

4.1. DMCA

DMCA predstavlja nadogradnju američkog zakona o autorskim pravima koji kriminalizira stvaranje i širenje tehnologija namijenjenih zaobilaženju sustava za zaštitu autorskih prava. Prema ovom zakonu, zaobilaženje tehnologije koja štiti određeni sadržaj je ilegalno ukoliko je počinjeno s namjerom nanošenja štete vlasniku autorskih prava.

Inverzni inženjering postojećih sustava dopušten je samo u točno određenim okolnostima, kao što je potreba za postizanjem kompatibilnosti s drugim programskim paketima. Primjena alata otvorenog programskog koda za dekriptiranje sadržaja zaštićenih CSS sustavom predstavlja značajnu poteškoću u primjeni DMCA zakona zbog toga što je legalnost takvog postupka vezana uz namjeru korisnika. Ako se dekriptiranje provodi s namjerom postizanja kompatibilnosti operacijskog sustava otvorenog programskog koda, ono je legalno. S druge strane, raspačavanje takvih programskih paketa s namjerom provođenja ili poticanja kršenja autorskih prava smatra se ilegalnim.

DMCA skupina zakona pokazala se neefikasnom: na Internetu su dostupni brojni programski paketi namijenjeni zaobilaženju sustava za upravljanje digitalnim pravima.

Iako zakoni dopuštaju iznimku u slučaju znanstvenog istraživanja, kriteriji koji opisuju takve slučajeve nisu jednoznačni. Zbog toga je donošenje DMCA zakona izazvalo snažnu reakciju unutar akademskih krugova koji se bave izučavanjem kriptografije. Mnogi znanstvenici strahuju kako istraživanja na polju kriptoanalize krše, ili bi mogla bit korištena za kršenje, DMCA zakona. Primjer takve zlouporabe zakona je uhićenje ruskog znanstvenika Dimitrija Skylarova 2001. godine nakon prezentacije na DEF CON konferenciji.

4.2. EUCD

EUCD direktiva, poznata još pod nazivom Infosoc (eng. *Information Society Directive*), donesena je u sklopu SEA (eng. *Single European Act*) izmjena Rimskog sporazuma, čiji cilj je formiranje jedinstvenog EU tržišta. U vrijeme nastanka, bila je to mjera za čije donošenje su na Europski parlament vršeni najveći pritisci od strane različitih lobističkih skupina. U svom konačnom obliku, EUCD direktiva definira uske granice slučajevima u kojima ja zaobilaženje DRM sustava dozvoljeno te se zbog toga njezino usvajanje smatra velikom pobjedom vlasnika autorskih prava, a na štetu korisnika.

Mnogi značajni detalji zakonskog okvira upravljanja digitalnim pravima nisu definirani ovom direktivom. Zemlje članice Europske Unije imaju zbog toga veliku slobodu u pojenim aspektima implementacije. Rastuća javna svijest o važnosti donošenja zakona vezanih uz zaštitu autorskih prava uzrokovala je u nekoliko slučajeva usporenje implementacije. Europska komisija pokrenula je čak i procese pred Europskim sudom pravde protiv šest zemalja članica koje su značajnije kasnile s implementacijom EUCD direktive (rok za implementaciju istekao je 22. prosinca 2002. godine).

5. Nedostaci DRM sustava

DRM tehnologije vlasnicima autorskih prava, ograničavanjem načina upotrebe, omogućuju kontrolu nad zaštićenim sadržajima. Samim time DRM sustavi predmet su brojnih kontroverzi. Naime, uvođenje ograničenja nad uporabom takvih sadržaja može predstavljati narušavanje zakonskih prava (eng. *fair use rights*) vlasnika legalnih kopija. DRM tehnologije meta su kritika i zbog toga što otežavaju, a u nekim slučajevima i potpuno onemogućuju, učinkovito arhiviranje sadržaja te povijesna istraživanja. Protivnici sustava za upravljanje digitalnim pravima ističu također kako ovi sustavi nisu učinkoviti u sprječavanju stvaranja ilegalnih kopija sadržaja koje bi trebali štititi, jer ni jedan DRM sustav nije, niti može biti, u potpunosti otporan na napade. Nakon probijanja zaštite samo jedne inačice nekog sadržaja, ili u slučaju kopiranja nezaštićene inačice, on postaje široko dostupan putem Interneta ili komercijalnog piratstva.

5.1. Metode zaobilaženja DRM sustava

Na raspolaganju su brojne metode zaobilaženja DRM sustava za zaštitu audio i video sadržaja.

5.1.1. Posredno kopiranje pomoću audio CD diska

Jedna od jednostavnijih metoda kopiranja audio sadržaja je njihovo snimanje na audio CD disk te kodiranje sadržaja tako dobivenog diska u željeni format bez DRM zaštite. Prilikom ovakvog kopiranja često dolazi do snižavanja kvalitete sadržaja jer korisnici uglavnom biraju formate koji koriste kompresiju uz gubitak podataka (eng. *lossy*), npr. pohranjivanje pjesama u MP3 datotekama umjesto u WAV datotekama. Na raspolaganju su programski paket koji automatiziraju snimanje zaštićene glazbe na prepisivi CD medij, ili na virtualni disk, te kodiranje sadržaja takvog diska u format bez zaštite. Postupak se automatski ponavlja dok nisu učinjene kopije svih odabranih pjesama, bez potrebe za sudjelovanjem korisnika u procesu. Primjer ovakve aplikacije je *NoteBurner M4P Converter*.

5.1.2. Kopiranje presretanjem toka podataka

Razvijeni su brojni programski paketi koji presretanjem toka podataka tijekom dekriptiranja DRM sadržaja omogućuju njihovo pohranjivanje u datoteke bez zaštite. Takve datoteke mogu sadržavati sadržaj istovjetan originalu (eng. *lossless*) ili mogu biti komprimirane uz određeni gubitak kvalitete.
Aplikacije koje provode opisani postupak zahtijevaju dekripcijski ključ. Programski paketi namijenjeni kopiranju DVD, HD-DVD i *Blu-Ray* diskova sadrže univerzalne dekripcijske ključeve dok aplikacije za kopiranje *TiVo ToGo*, *iTunes* i *PlayForSure* sadržaje zahtijevaju korisnikov dekripcijski ključ. Potonje aplikacije omogućuju dakle kopiranje sadržaja koje je korisnik legalno kupio putem vlastitog korisničkog računa.
Neki od programskih paketa koji omogućuju kopiranje DRM sadržaja presretanjem toka podataka tijekom dekripcije su: *QTFairUse* i *MyFairUse* za *iTunes* pjesme, *RipIt4Me* i *DVD Fab Decrypter* za DVD diskove te *FairUse4Wm* za *PlaysForSure* sadržaje.

5.1.3. Analogna rupa

Svi oblici DRM sustava za zaštitu audio i video sadržaja imaju ranjivost slikovitog naziva analogna rupa (eng. *analog hole*). Naime, kako bi korisnik mogao konzumirati takve sadržaje digitalni signali moraju se pretvoriti u analogne signale koji sadrže svjetlosne i/ili zvučne komponente. Takvim analognim signalom moguće je po volji rukovati jer DRM sustavi nad njima nemaju nikakve kontrole.
Sve današnje sustave za upravljanje digitalnim pravima, a vjerojatno i sve buduće sustave, moguće je zaobići snimanjem analognih signala, njihovim digitalizacijom u format bez zaštite te distribucijom. Nedostatak ove skupine metoda je gubitak kvalitete sadržaja prilikom uzastopne digitalno-analogne i analogno-digitalne pretvorbe.

5.1.4. DRM sustavi na računalima opće namjene

Mnogi aktualni DRM sustavi oblikovani su za upotrebu na računalima opće namjene, kao što su tzv. PC osobna računala, zbog toga što su takva računala percipirana kao glavni uzrok gubitka profita uzrokovanog neovlaštenim kopiranjem. DRM programski paketi moraju sadržavati sve informacije

potrebne za reprodukciju sadržaja, kao što su npr. dekripcijski ključevi, pa zbog toga nikad ne mogu biti potpuno sigurni. Uvijek postoji mogućnost otkrivanja takvih informacija što potom omogućuje dekriptiranje sadržaja i njegovo kopiranje.

5.1.5. DRM sustavi za namjensko sklopovlje

Mnogi DRM sustavi koriste kriptirane medije koji zahtijevaju posebno oblikovano sklopovlje za reprodukciju. Na ovaj se način pokušava osigurati da samo ovlašteni korisnici, tj. vlasnici spomenutog sklopovlja, mogu pristupiti sadržaju. Namjenskim uređajima također se pokušava sačuvati tajnost dekripcijskih ključeva.
Iako ovakvi sustavi u načelu osiguravaju sadržaje od neovlaštenog rukovanja, razvoj uređaja koji bi uspješno skrivao ključeve za dekripciju u praksi se pokazao kao izrazito težak zadatak. Niti jedan ovakav sustav nije izdržao više od nekoliko godina eksploatacije. Nakon otkrivanja tajnog ključa najčešće je jednostavno izgraditi inačicu uređaja koji prilikom reprodukcije ne provodi provjeru legalnosti kopije.

5.1.6. Digitalni vodeni žigovi

Digitalne vodene žigove najčešće je jednostavno ukloniti, iako ponekad uz degradaciju video ili audio sadržaja. Na primjer, većina kompresijskih algoritama oblikovana je tako da zadrže vidljive značajke slike. Ako je digitalni vodeni žig nevidljiv, nuspojava kompresije najčešće je njegovo uklanjanje.

6. Zaključak

Tehnologije za upravljanje digitalnim pravima imaju temeljni nedostatak koji ih efektivno čini neučinkovitima. Naime, da bi takvi sustavi imali smisla njihovi tvorci krajnjem korisniku moraju omogućiti konzumiranje zaštićenih sadržaja, odnosno moraju mu omogućiti pristup svim alatima i informacijama potrebnim za reprodukciju. Nakon predaje kriptografskog algoritma, ključeva i kriptiranog sadržaja korisnicima, samo je pitanje vremena kada će doći do kompromitiranja sustava.
Brojni eksperimenti, istraživanja i iskustva iz prakse pokazala su kako DRM sustavi nisu učinkoviti. Svaki sadržaj zaštićen u legalnoj distribuciji nekom od aktualnih DRM tehnologija dostupan je putem Internet servisa za razmjenu datoteka ili na ilegalnim prodajnim mjestima komercijalnih pirata. Istraživanja su pokazala kako izdavači i autori mogu više zaraditi besplatnom podjelom knjiga jer omogućavanje skidanja neke knjige na Internetu povećava prodaju, ne samo ostalih knjiga istog autora, već, iznenađujuće, i naslova koji je besplatno dostupan. Slično vrijedi u glazbenoj industriji.
Postavlja se pitanje koji je smisao ulaganja velikih novčanih iznosa te ljudskih resursa u razvoj i implementaciju tehnologije koja je po samoj svojoj definiciji osuđena na neuspjeh. Osim toga, korisnicima, koji sadržaj ne žele platiti, uvijek će na raspolaganju stajati ilegalni načini stjecanja inačica sadržaja bez zaštite. S druge strane, korisnici koji su svoje inačice legalno pribavili osuđeni su prilikom rukovanja tim sadržajima na sva ograničenja koja DRM sustavi donose.

7. Reference

[1] Digital rights management, http://en.wikipedia.org/wiki/Digital_Rights_Management, listopad 2007.
[2] Digital Rights Management, Final Report, http://europa.eu.int/comm/enterprise/ict/policy/doc/drm.pdf, listopad 2007.
[3] Perer Seebach: Standards and specs: Digital rights management: When a standard isn't, http://www-128.ibm.com/developerworks/power/library/pa-spec11/?ca=dgr-lnxw06StandardDRM, listopad 2007.
[4] Hagai Bar-El: Challenges in Designig Content Protection Solutions, http://www.hbarel.com/publications/Challenges_in_designing_content_protection_solutions.pdf, listopad 2007.
[5] Lawrence Lessig: Free Culture, http://www.free-culture.cc/freeculture.pdf, listopad 2007.
[6] Customer's Guide to DRM, http://www.indicare.org/tiki-page.php?pageName=ConsumerGuide, listopad 2007.
[7] Content Scramble System, http://en.wikipedia.org/wiki/Content_Scrambling_System, listopad 2007.
[8] Stream cipher, http://en.wikipedia.org/wiki/Stream_cipher, listopad 2007.
[9] Protected Media Path, http://en.wikipedia.org/wiki/Protected_Media_Path, listopad 2007.
[10] FairPlay, http://en.wikipedia.org/wiki/FairPlay, listopad 2007.
[11] Directive on the harmonisation of certain aspects of copyright and related rights in the information society, http://en.wikipedia.org/wiki/European_directive_on_copyright, listopad 2007.