

ZAŠTITA AUTORSKIH PRAVA DIGITALNIH SADRŽAJA

ZORAN SAVIĆ

Fakultet za menadžment, Novi Sad

MARKO POPOVIĆ

Fakultet za menadžment, Novi Sad

Rezime: Digitalna revolucija, koja je omogućila korisnicima da koriste digitalne sadržaje na potpuno novi način, kao i sama priroda digitalnih sadržaja, koja omogućuje njihovo kopiranje i distribuciju na jednostavan i jeftin način, doprineli su da je kontrola distribucije tih sadržaja veoma otežana, a zaštita autorskih prava izdavača, proizvođača i ostalih nosilaca tih prava, postala je poseban problem.

Poseban vid narušavanja autorskih prava je softverska piraterija, o kojoj postoje dijametralno suprotni stavovi u stručnim krugovima, ali i u pravnim tumačenjima i praktičnom ponašanju nekih institucija i država.

U radu su date aktuelne definicije sistema za upravljanje digitalnim pravima, kao i kraći istorijski pregled korišćenih sistema u različitim oblastima distribucije digitalnih sadržaja (muzika, film, računarski softver itd).

Opisana su i neka zakonska rešenja, koja regulišu ovu oblast, kako u svetu, tako i u Srbiji, a u tom kontekstu prikazani su i stavovi protivnika primene ovih sistema.

Analiza postojećeg stanja ukazuje na potrebu kreiranja takvog koncepta sistema za upravljanje digitalnim pravima, koji bi mogao da zaštiti ekonomske interese njihovih nosilaca, a koji bi istovremeno bio jednostavan za upotrebu i ne bi narušavao potrošačka prava korisnika tih sadržaja. U tom smislu, u radu su prikazani mogući pristupi u definisanju arhitekture ovakvih sistema.

Ključne reči: (autorska prava) copyright, (intelektualna svojina) intellectual property, (digitalni sadržaj) digital content, (upravljanje digitalnim pravima) digital rights management

1. UVOD

Digital rights management (DRM) je termin koji se koristi za opis tehnologija kontrole pristupa, koje koriste kompanije kao što su Sony, Amazon, Apple Inc., Microsoft, AOL i BBC, ali i drugi proizvođači, izdavači, nosioci autorskih prava i pojedinci, da bi na neki način ograničili neovlašćeno, i kontrolisali dozvoljeno korišćenje digitalnih sadržaja. DRM podrazumeva sve načine kontrole pristupa zaštićenom digitalnom sadržaju pomoću savremenih tehnologija. U suštini, kontrola korišćenja tog sadržaja je, umesto u rukama njegovog vlasnika, autora ili izdavača, poverena određenom softveru. Pri tome se koriste različite metode, zavisno od toga da li se radi o video ili muzičkim sadržajima, tekstualnim dokumentima, običnim porukama elektronske pošte, ili bilo kojim drugim osetljivim digitalnim sadržajima, koji treba da budu zaštićeni od neovlašćenog korišćenja.

Iako mnogi korisnici DRM metode, posebno one koje se primenjuju u filmskoj i muzičkoj industriji, smatraju previše restriktivnim, njima se zapravo pokušava da reši jedan zakonski problem – zaštite autorskih prava, koja su značajno narušena, u poslednje vreme, neovlašćenom distribucijom digitalnih sadržaja putem interneta. Svako preuzimanje MP3 muzike ili filma, sa neke od takozvanih P2P (peer-to-peer) mreža, znači gubitak za njihove autore i distributere. Neke procene ukazuju da, samo u filmskoj industriji, to donosi gubitak od skoro 5 milijardi dolara na godišnjem nivou.

Zbog prirode Interneta je potpuno nepraktično pokretanje sudskog postupka protiv svakog ko na taj način krši zakon, pa je autorima i distributerima preostalo da, pomoću određenih tehnoloških rešenja, pokušaju da spreče neovlašćeno kopiranje svojih dela u digitalnom formatu.

Pri tome, poseban problem predstavlja zahtev da se legalnim korisnicima (ili kupcima) tih digitalnih sadržaja omogući da prave kopije za sopstvene potrebe, što je suština doktrine "odgovarajućeg korišćenja" (*fair use*) karakteristične za propise o zaštiti autorskih prava. Međutim, ovu doktrinu je teško sprovesti DRM metodama, jer računarski program teško može da odluči šta predstavlja "odgovarajuće korišćenje".

Relativno je jednostavno napraviti sistem koji će moći da kontroliše korisnička prava tipa "dozvoljena su 2 kopiranja", jer računar može da razume šta je broj 2, ali ne može da razume iskaze poput "kopirao sam sadržaj na moj laptop i MP3 plejer, a sada imam novi računar na koji bi trebalo ponovo da kopiram". Uslovi "odgovarajućeg korišćenja" ne mogu lako da se digitalizuju. Mnoge kompanije su, u cilju zaštite svojih prava, eliminisale bilo kakvu mogućnost odlučivanja korisnika o pravima korišćenja isporučenog sadržaja.

DRM tehnologije pokušavaju da kontrolišu korišćenje sadržaja digitalnih medija sprečavanjem krajnjih korisnika da neovlašćeno koriste, kopiraju ili konvertuju te sadržaje u drugi format. Na neki način to jeste zaštita autorskih prava, poznata još pre pojave digitalnih medija, a koja razvojem tehnologije dobija sve više na značaju, jer načini narušavanja ovih prava postaju sve jednostavniji (od kopir aparata, magnetofona, kasetofona, videorikordera, do personalnih računara). Dolazak digitalnih medija i tehnologija analogno-digitalne konverzije, uz masovno korišćenje personalnih računara, napravio je pravu paniku u filmskoj i muzičkoj industriji, čiji prihodi su bili najugroženiji. Naime, dok sadržaji na analognim medijima po pravilu gube na kvalitetu kopiranjem, to nije slučaj sa sadržajima na digitalnim medijima. Mogućnosti personalnih računara, uz pojavu Interneta i alata za razmenu podataka na internetu, znatno su olakšale neautorizovanu distribuciju autorskim pravima zaštićenih digitalnih sadržaja – koju mnogi nazivaju i digitalna piraterija.

DRM tehnologije su upravo nastale sa pokušajem da se spreči digitalna piraterija, ali

su često sprečavale i normalno korišćenje (*fair use*) zaštićenih, ili čak i nezaštićenih digitalnih sadržaja.

Cilj ovog rada je da pruži širi uvid u aktuelno stanje u ovoj oblasti, kao i da ukaže na moguće pravce daljeg razvoja DRM sistema.

2. ZAKONSKA REGULATIVA

Primena DRM sistema je od početka naišla na potpuno oprečne reakcije. Sa jedne strane su kompanije, proizvođači i distributeri digitalnih sadržaja, koje se na taj način štite od narušavanja autorskih prava, štite svoju intelektualnu svojinu i, u krajnjoj liniji, svoje prihode. Digitalna zaštita je, po njima, neophodna za sprečavanje krađe intelektualne svojine, kao što su fizičke zaštite (brave) neophodne da bi se zaštitila lična svojina. Sa druge strane, protivnici DRM-a (*Free Software Foundation*, *Electronic Frontier Foundation*) tvrde da se tako guše inovativnost i slobodna konkurencija i da digitalne zaštite, koje se koriste u DRM, mogu da ograničavaju korisnike i kada su u pitanju sasvim legalne aktivnosti, poput kopiranja CD ili DVD za svoje potrebe, iznajmljivanja materijala u bibliotekama, ili korišćenju tog materijala u naučnim istraživanjima i obrazovanju. Po njima, nosioci autorskih prava ograničavaju korišćene digitalnih sadržaja na način koji nije u skladu sa zakonom o autorskim pravima u drugim oblastima. Oni tvrde da je korisnik taj koji treba da bude zaštićen zakonom jer, na ovakav način primenjen, DRM nije akronim za *digital rights management*, nego za *digital restrictions management* [1].

DRM sistemi su dobili određenu zakonsku potporu u nekoliko međunarodnih akata. Prvi je bio *WIPO Copyright Treaty* (WCT) iz 1996. godine, koji su prihvatile većina zemalja, članica međunarodne organizacije za zaštitu intelektualne svojine *World Intellectual Property Organization*, a čiji Član 11 zahteva od svih nacionalnih organizacija da donesu zakone protiv pokušaja zaobilazanja DRM sistema [2].

U SAD, to je učinjeno putem *Digital Millennium Copyright Act* (DMCA), dok je u Evropi ovaj ugovor ugrađen u *European directive on copyright*, iz 2001. godine, koji zahteva od zemalja članica EU da uvedu zakonsku zaštitu preventivnih tehničkih zaštitnih mera (odnosno DRM).

DMCA je dodatak Zakona o autorskim pravima SAD, kojim se nezakonitim proglašava proizvodnja i širenje tehnologija koje omogućavaju korisnicima da na neki način zaobiđu tehničke mere za ograničavanje kopiranja, a sa osnovnim ciljem narušavanja autorskih prava njihovih legitimnih nosilaca. Pri tome, naglasak je stavljen na namere, odnosno ciljeve eventualnog prekršioca. Ovo je otvorilo dosta rasprava, pošto je, na primer, svaki reverzni inženjering (dekriptovanje DRM sistema), učinjen radi postizanja interoperabilnosti između komercijalnih i takozvanih otvorenih operativnih sistema, ovim aktom dozvoljen, ali nije dozvoljena dalja distribucija tog softvera za dekripciju koja bi omogućila drugima narušavanje autorskih prava [3].

DMCA se pokazao prilično neefikasnim, kada je u pitanju zaštita DRM sistema [4], ali je zato imao negativan uticaj na razvoj kriptografije, zbog straha istraživača da bi određenim kriptanalizama mogla biti narušena neka njegova odredba. Na primer, na osnovu ovog akta, jedan ruski programer je 2001. godine uhapšen u SAD i proveo je nekoliko meseci u zatvoru, posle prezentacije jednog programa za dekripciju elektronskih knjiga, izvršene na konferenciji *DEFCON* u Las Vegasu. Primena ovog akta je naročito nailazila na otpor studenata koji su se bavili kriptanalizom, kao i konsultanata u domenu računarske bezbednosti. Holandski stručnjak, *Niels Ferguson*, odbio je da objavi informacije o ranjivosti jednog Intelovog sistema, u strahu da bi, na osnovu DMCA, mogao da bude uhapšen kada otputuje u SAD.

Aprila 2007. godine, Evropski parlament je podržao direktivu EU iz 2001. godine [5], u cilju usklađivanja krivičnih zakona u zemljama članicama EU, čime bi se one obavezale da kažnjavaju, novčano i zatvorski

– zavisno od težine prekršaja, svako narušavanje intelektualnih prava, nastalo iz komercijalnih razloga. Znači kopiranje iz nekomercijalnih razloga i za lične potrebe je isključeno iz ove direktive.

Ovom problematikom, naročito sa aspekta iznalaženja mogućnosti zadovoljavanja različitih interesa svih korisnika DRM sistema bavio se i evropski međunarodni projekat INDICARE, kao i FP6 projekat AXMEDIS [6,7].

Sa jedne strane, velike filmske, muzičke i softverske kompanije pokušavaju da spreče milione korisnika različitih *torrent* aplikacija da razmenjuju i dele sadržaje preko interneta, jer veliki deo tih sadržaja čine piratske kopije. Sa druge strane, internet korisnici se opiru i traže fleksibilniju zakonsku regulativu koja će biti u skladu sa slobodarskom prirodom interneta.

Tako je februara 2008. godine osnovana *Piratska partija Srbije* (PPS), kao jedna od četrdesetak "sestara" *Međunarodne piratske partije* (PPI), od kojih je oko dvadeset službeno registrovano u svojim zemljama i koja ima čak i jednog predstavnika u Evropskom parlamentu, jednog u parlamentu Tunisa i niz predstavnika u vlasti na lokalnom nivou u raznim evropskim zemljama. Ovaj međunarodni pokret, čiji je cilj povezivanje i promocija piratskih partija širom sveta, traži reformu zakona koji se tiču zaštite autorskih prava, veće pravo privatnosti na internetu i u realnom životu, kao i transparentnost delovanja državnih administracija [8]. Oni zahtevaju pravo da "slobodno i bez ograničenja komuniciramo preko interneta preporučujući linkove za preuzimanje određenih sadržaja, kao što imamo pravo da govorimo o čemu god želimo. Razmena linkova nije isto što i prodaja piratskih diskova na ulici, jer linkovanjem niko ne zarađuje, niko nije oštećen. Hapšenje i kazne zbog razmene podataka na internetu predstavljaju represiju i rušenje osnovnih vrednosti savremenog društva".

Razmena sadržaja korišćenjem P2P (*peer to peer*) umrežavanja nije na jedinstveni način

regulisana ni u Evropskoj uniji, a napredak tehnologije neke direktive donete pre desetak godina čini jednostavno zastarelim. Tako je, na primer, u Rusiji preuzimanje filmova i muzike "za kućnu upotrebu" besplatno, u Kanadi i Holandiji to važi samo za muziku, a u Francuskoj internet provajder ima pravo da isključi korisnika, za koga ustanovi da se bavi ovom aktivnošću, tek posle dve opomene.

U Srbiji, tu problematiku donekle pokrivaju *Krivični zakon Srbije* i *Zakon o autorskim i srodnim pravima*, ali se otkrivanje prekršilaca često kosi sa *Zakonom o zaštiti podataka o ličnosti* [9].

3. OSPORAVANJA

Ne postoje opšte prihvaćeni standardi za DRM. Mnoge kompanije iz sveta digitalne zabave koriste nešto restriktivniji pristup, koji korisnicima apsolutno ne dozvoljava kopiranje, štampanje, izmenu ili slanje digitalnog materijala. Ovakav pristup često prevazilazi potrebe zaštite autorskih prava i zbog toga je predmet osporavanja mnogih korisnika, al i biblioteka i obrazovnih institucija. Biblioteke ne mogu da čuvaju softver sa vremenski ograničenim ključem za enkripciju i ne mogu na uobičajeni način iznajmljivati sadržaj koji je licenciran za određenu računarsku konfiguraciju.

Argumenti protiv DRM su moguće narušavanje privatnosti korisnika, nemogućnost pravljenja kopija za svoje potrebe, pravo korisnika da preproda ili pokloni sadržaj koji je kupio, zastarevanje zaštite posle izvesnog vremenskog perioda, nemogućnost promene hardvera bez narušavanja licencnih uslova itd.

Po nekima, DRM utiče i na slobodu govora. Primer za to je pretnja tužbama mnogih kompanije iz muzičke industrije profesoru Edvardu Feltenu sa *Princeton* Univerziteta, koji je 2001. godine pokušao da objavi članak o lošim DRM sistemima, jer bi njegova istraživanja mogla da omoguće korisnicima da izbegnu tu zaštitu [10].

Mnogo je organizacija, naučnika i eminentnih pojedinaca koji se protive primeni DRM, kao što su suosnivač kompanije *Autodesk*, John Walker [11], osnivač pokreta slobodnog softvera Ričard Stallman [12], i profesor Ross Anderson sa Kembridž univerziteta, koji predvodi britansku organizaciju koja se suprotstavlja DRM inicijativama u UK i šire. Čak je i Bil Gejts imao primedbi na DRM, jer po njemu, ne obavlja dobro svoj zadatak i prouzrokuje više problema legalnim korisnicima [13].

Organizacije kao što su *Electronic Frontier Foundation*, *Free Software Foundation* i slične organizacije su među najeksponiranijim protivnicima DRM. Konačna verzija *GNU General Public License*, verzija 3, izdata od strane *Free Software Foundation*, omogućuje izbegavanje DRM-a, bez kršenja odredbi DMCA. Maja 2006. godine, FSF je pokrenuo kampanju protiv DRM, pod nazivom "*Defective by Design*" [14,15].

Association for Computing Machinery (ACM) i *Institute of Electrical and Electronics Engineers (IEEE)* su takođe protivnici DRM.

Osnovni argumenti oponenta su da je u svim DRM sistemima mnogo više značaja dato zabranama nego pravima korisnika, odnosno da se njihovo funkcionisanje kosi sa pravima potrošača, da narušavaju prava raspolaganja privatnom svojinom i da ograničavaju legalne aktivnosti korisnika, ograničavajući funkcionisanje njihovih uređaja za reprodukciju na osnovu vrste sadržaja koji se na njima reprodukuje [16].

Onemogućavanje pravljenja ličnih ili bibliotečkih kopija, pozajmljivanja prijateljima ili čak i nasleđivanja, samo su neki od argumenata protiv DRM.

Stručnjak za računarsku bezbednost *Bruce Schneier* nameru zabavne industrije da sprečavanjem kopiranja sačuva svoje postojeće poslovanje, naziva nemogućim poduhvatom, osuđenim na neuspeh. Pokušaji pravljenja digitalnih fajlova koji se ne mogu kopirati je kao " pravljenje vode koja nije vlažna" [17].

Upravo zbog navedenih protivljenja, mnoge kompanije i izvođači u industriji zabave su prestali da koriste DRM sisteme i čak počeli da reklamiraju svoje proizvode kao "DRM-Free".

Iz prethodne analize se vidi da primena i poštovanje zakona i propisa koji se odnose na DRM nije jednostavna stvar, a ugovorni odnosi između prodavaca i korisnika ne mogu se brzo i lako definisati, tako da je i korisniku teško da odredi u kom trenutku su zakoni prekršeni. Na primer, da li je prekršaj narezivanje muzičkog CD, pozajmljivanje kupljenog ili narezanog CD prijatelju, njegova preprodaja, itd. To je jedan od razloga zbog koga svakog dana milioni korisnika interneta, samo razmenom muzike, na neki način krše zakone o autorskim pravima.

Ponekad je narušavanje autorskih prava, naročito kada je u pitanju kopiranje softvera, od koristi za proizvođača tog softvera, zbog širenja korisničke baze, a malih realnih gubitaka.

Zbog toga je problem zaštite autorskih prava, naročito kada je distribucija muzičkih sadržaja preko interneta u pitanju, pored primene različitih sistema zaštite, dovela i do potrebe za promenom načina poslovanja izdavačkih kompanija i on line prodavnica.

Jedan od načina je omogućavanje lakog i jeftinog preuzimanja, jer su mnogi nekomercijalni sajtovi za preuzimanje muzike složeni za korišćenje, spori i predstavljaju rasadnike zlonamernih programa koji se dobijaju u paketu sa željenim muzičkim sadržajem. Ako su sve pesme raspoložive na jednom tehnički korektnom sajtu, po razumnim cenama, može se očekivati da će se korisnici pre odlučivati za njega, nego za sajt sa besplatnom muzikom, ali nelegalan, spor i pun virusa.

Besplatno preuzimanje muzike na internetu omogućuju i mnogi izvođači u cilju skretanja pažnje na nova izdanja i njihovu kasniju kupovinu, eliminacije posrednika u prodaji, ili promocije koncertnih aktivnosti, kojima mogu

da nadomeste gubitke nastale slobodnom distribucijom muzike. Naravno da izdavačke kuće, koje prihod zasnivaju na prodaji albuma, nisu velike pristalice ovakvog poslovnog modela.

4. OBLASTI PRIMENE

Razvoj i primena određenih DRM tehnologija su u velikoj meri zavisili i od oblasti u kojoj je bila potrebna kontrola korišćenja digitalnih sadržaja. DRM je najčešće korišćen u industriji zabave (muzika, film, televizija), a u poslednje vreme naročito i u industriji softvera.

DRM, kada je reč o zabrani kopiranja, nije nov koncept (specijalno zaštićeni flopi ili kompakt diskovi, hardverski dodaci – hardlok, bez kojih bi sadržaj bio neupotrebljiv itd, postoje već duže vreme), pa bi savremeni DRM sistemi pored zabrane kopiranja trebali da ponude i neke druge mogućnosti i da omoguće čvršću povezanost izdavača i korisnika.

Uobičajene tehnike DRM su restriktivni licencni ugovori (kojima se uslovljava korišćenje ili preuzimanje digitalnih sadržaja sa određenih sajtova) i enkripcija (kojom se kontroliše pristup i reprodukcija digitalnog sadržaja, uključujući i pravljenje rezervnih kopija za svoje potrebe) [18].

Jedna od najranijih implementacija DRM je bio *Software Service System* (SSS), osmišljen od strane japanskog inženjera *Ryoichi Mori*, 1983. godine, kasnije doradivan pod nazivom *superdistribucija*. SSS je bio zasnovan na enkripciji sadržaja, uz korišćenje specijalizovanog hardvera za dekrpciju i sa mogućnošću plaćanja nosiocu prava. Osnovni princip ovog sistema je neograničena distribucija enkriptovanih digitalnih sadržaja [19].

Film

Jedan od prvih primera DRM sistema je bio *Content Scrambling System* (CSS) razvijen 1996. godine od strane *DVD Forum*a za filmove na DVD medijima. CSS je koristio jednostavan algoritam za enkripciju i zahtevao

je od proizvođača uređaja za reprodukciju da potpišu licencni ugovor, kojim se ograničavaju mogućnosti tih uređaja koje bi dozvolile pravljenje digitalnih kopija. Međutim, pojavom DeCSS programa 1999. godine, omogućena je reprodukcija CSS enkriptovanih DVD filmova na računarima koji su koristili Linux platformu.

Microsoft je u svoju Windows platformu ugradio DRM sistem pod nazivom *Protected Media Path*, koji sadrži *Protected Video Path* (PVP). PVP pokušava da spreči DRM-om zaštićen sadržaj da se reprodukuje, ako se istovremeno izvršava neki softver nepoznatog porekla, a koji bi mogao da pristupi tom sadržaju. Pored toga, PVP može da enkriptuje informacije za vreme njihovog prenosa do monitora ili grafičke kartice, što još više otežava neautorizovano kopiranje (snimanje).

Advanced Access Content System (AACS) je DRM sistem za HD DVD i Blu-ray diskove razvijen od strane AACS Licensing Administrator (AACS LA) konzorcijuma koji čine *Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Brothers, IBM, Toshiba i Sony*. Decembra 2006. godine, hakeri su na internetu objavili ključ za enkripciju, omogućivši na taj način neograničeni pristup AACS zaštićenom HD DVD sadržaju. Usledila je promena ključeva od strane AACS, ali su i oni ubrzo bili krekovani [20].

Neka DRM rešenja, prilikom DVD zaštite, koriste slabosti softvera za "narezivanje" u cilju sprečavanja kopiranja diskova. Na DVD se snimi mali programski kod, koji, koristeći uočene slabosti DeCSS koda na kojima se zasniva većina programa za kopiranje, zaustavlja process kopiranja. Naravno, ova zaštita nije efikasna ako softver za kopiranje nije baziran na DeCSS. Iako *Digital Millennium Copyright Act* iz 1998. godine, u SAD zabranjuje onemogućavanje funkcionisanja DRM sistema, na hiljade ljudi to aktivno radi i objavljuje metode kojima se to postiže.

Po ovom aktu, zabranjeno je i kreiranje, naručivanje ili preuzimanje bilo kog proizvoda koji omogućuje zaobilaženje DRM restrikcija.

Razna udruženja za zaštitu potrošača zahtevaju dopunu ovog akta, jer on nosiocima prava daje po njima nekorektnu prednost, ne ograničavajući ih na bilo koji način u primeni bilo kakvog DRM sistema.

TV

U SAD je korišćen *CableCard* standard od strane provajdera kablovske TV, u cilju omogućavanja pristupa određenim kanalima samo pretplaćenim korisnicima [21].

Koncept *broadcast flag* je razvijen od strane *Fox Broadcasting*-a 2001. godine i podržan je od strane *Motion Picture Association of America* (MPAA) i *Federal Communications Commission* (FCC). Posle dosta osporavanja, naročito zbog problema koje je činio korisnicima koji su hteli da snime sadržaje koje će gledati u terminima koji im više odgovaraju, uspešnije je primenjen tek prihvatanjem od strane *Digital Video Broadcasting Project* konzorcijuma (DVB), koji su činili 250 stanica, proizvođača, mrežnih provajdera, softverskih kompanija i regulacionih tela iz 35 zemalja, sa pokušajem keiranja novih standarda za digitalnu televiziju. U Evropi je 2007. godine razvijena varijanta ovog rešenja - *Content Protection and Copy Management* (DVB-CPCM), koja kao i većina DRM rešenja kontroliše korišćenje zaštićenog materijala, po uputstvima vlasnika prava nad tim materijalom. Iako je normativno zaživeo kao standard (ETSI TS 102 825-X), još nema njegove pune implementacije od strane proizvođača uređaja (jer još niko ne daje sertifikate) [22].

Muzika

Diskovi koji su koristili neki od DRM sistema nisu mogli da se reprodukuju na svim CD plejerima, ili računarima, čime nisu zadovoljavaju standard za audio diskove (poznat kao *Red Book* standard).

Sony BMG je 2005. godine najvio novi DRM sistem koji je bez obaveštenja i dozvole instalirao DRM softver na računar korisnika, a koji je, između ostalog, sadržao i skriveni

program, poznat i kao *rootkit*, koji omogućuje privilegovani pristup računarskim resursima, čineći na taj način računar korisnika osjetljivim na moguće zlonamerne napade. Posle velike bure koja se podigla ovom prilikom, a i zbog slabe efikasnosti ovog sistema, Sony je bio prinuđen da definitivno povuče ovo rešenje [23].

Januara 2007. godine, kompanija *EMI* je prestala sa izdavanjem audio diskova sa DRM, jer je procenjeno da troškovi primene DRM nisu praćeni odgovarajućim rezultatima, a njihov primer su sledila i još četiri muzička izdavača [24].

Internet muzika

Mnoge on line muzičke prodavnice koriste neki oblik DRM da bi na neki način ograničile korišćenje poručene i preuzete muzike sa interneta

- Do 2009. godine, Apple-ova prodavnica *iTunes Store* koristila je *FairPlay* DRM sistem za distribuciju muzičkih sadržaja, da bi ga kasnije zbog konkurencije napustila i zadržala samo za distribuciju video sadržaja i softverskih aplikacija..
- *Napster music store* nudi DRM sistem koji se zasniva na pretplati, tako da njihovi pretplatnici mogu da preuzimaju neograničenu količinu muzike u *Windows Media Audio* (WMA) formatu. Istekom pretplate, sva preuzeta muzika postaje neupotrebljiva, dok se pretplata ne obnovi. Posebno se naplaćuje korišćenje preuzete muzike na portabl uređajima, ili mogućnost snimanja (narezivanja) na CD. Uređaji koji mogu da reprodukuju muziku preuzetu sa Napstera nose *Microsoft PlaysForSure* logo (koji inače nemaju ni *iPod* plejeri, a čak ni plejer *Zune* kompanije Microsoft). Od juna 2009. godine i Napster daje bez DRM ograničenja muziku u MP3 formatu, koja se može slušati na iPhone-u i iPod-u..
- *Wal-Mart Music Downloads*, on line prodavnica muzike, naplaćuje \$0.94 po pesmi svako preuzimanje, pri čemu je reprodukcija moguća na svakom *Windows PlaysForSure* obeleženom proizvodu,

stim što kod nekih MP3 plejera mora sadržaj da bude snimljen u internu memoriju, a ne može reprodukcija da se vrši preko SD kartice.

- Sony je koristio sopstveni DRM sistem *OpenMG*, u svojoj prodavnici "Connect", koji je dozvoljavao reprodukciju sadržaja samo na računarima sa MS Windows operativnim sistemom i Sony hardverom (uključujući i Playstation i neke Sony Ericsson telefone).
- *Kazaa* nudi sistem pretplate, a preuzeti muzički sadržaji mogu se reprodukovati samo na uređajima koji poseduju Windows Media Player, onoliko dugo koliko je korisnik pretplaćen na ovaj servis.

Ovi različiti servisi nisu interoperabilni, čak iako koriste iste DRM sisteme. Skoro svi zahtevaju i preuzimanje nekog klijentskog softvera, i/ili *plug-in*, malu softversku komponentu koja povećava mogućnosti neke veće softverske aplikacije. Malo ih je kompatibilno i sa jednim od najmasovnijih prenosivih uređaja za reprodukciju muzike - Apple iPod.

Mada DRM preovlađuje kada je u pitanju Internet muzika, neke on line prodavnice (*Amazon*, *eMusic* itd) ga ne koriste, iako su protiv besplatnog deljenja muzike među korisnicima. A neki prodavci čak ohrabruju svoje kupce da preuzetu muziku međusobno dele, da bi se povećala popularnost izvođača. Sve više izdavača odustaje od DRM kada su u pitanju on line distribucije, jer shvataju da ne mogu da imaju kompletnu kontrolu nad celim on line muzičkim tržištem, i odlučuju se za prodaju muzike koja će moći da se reprodukuje na bilo kom digitalnom audio plejeru. *eMusic* upravo to radi i to mu je donelo drugu poziciju na tržištu, odmah iza *iTunes* [25].

U svom otvorenom pismu *Steve Jobs* je pozvao muzičku industriju da eliminiše DRM, a *Musicload.de*, jedan od najvećih evropskih on line prodavaca muzike, još 2007. godine se izjasnio protiv DRM, jer služba za podršku korisnicima tri četvrtine svog

vremena troši na rešavanje problema vezanih za DRM [26].

Računarske igrice

Računarske igrice ponekad koriste DRM da bi se ograničio broj sistema na koje ta igrice može da se instalira, zahtevajući autentifikaciju preko on line servera. Većina igrice dozvoljava tri do pet instalacija, što može da predstavlja problem ako korisnik menja računar, neki deo računara, ili reinstalira operativni sistem, jer igrice može da postane neupotrebljiva posle određenog broja instalacija, čak iako je koristi jedan korisnik na jednom računaru. Posledice toga su, najčešće, korišćenje piratskih kopija.

Mnogi proizvođači igrice pokušavaju da koriste neku vrstu on line DRM-a (na primer, *SecuROM*), tako što korisnik tokom igre mora da postepeno preuzima dalje delove igrice sa servera proizvođača. Međutim, ti serveri su posebno izloženi hakerskim napadima (primeri Ubisoft Uplay servera u martu 2010. godine i Sony PSP servera u aprilu 2011. godine).

E-knjige

Elektronska izdanja knjiga (*e-books*) koja se čitaju na računaru ili posebnom čitaču, koriste DRM da bi se ograničila mogućnost kopiranja, štampanja i deljenja tih izdanja.

Postoji četiri osnovna formata elektronskih knjiga. To su PDF, *Mobipocket*, *Topaz* i *ePub*. Neki uređaji podržavaju više formata (Amazon Kindle), a neki samo *ePub* format, koristeći pri tome različite DRM šeme (Adobe's Adept DRM, Apple's Fairplay DRM, Barnes & Noble's, Amazon's DRM).

Čitanje e-knjiga omogućuju dva programa *Adobe Reader* i *Microsoft Reader*, svaki sa svojom verzijom DRM. Kod Adobe sistema, zavisno od vrste e-knjige, korisniku (ni)su na raspolaganju određene funkcije (print, copy, paste), što mu se po otvaranju knjige daje do znanja. Nivo ograničenja određuje izdavač ili prodavac.

Microsoft Reader, koji čita e-knjige u .lit formatu, koristi tri nivoa kontrole pristupa: *sealed e-books* (najmanja ograničenja, zabranjena je samo izmena sadržaja), *inscribed e-books* (sprečava dalju distribuciju knjige instalacijom ID taga kojim se identifikuje prvi vlasnik) i *owner exclusive e-books* (najrestriktivniji – koji dozvoljava čitanje knjige samo na računaru pomoću koga je preuzeta sa interneta, uz zabranu kopiranja i distribucije) [27].

Problem sa ovom vrstom DRM je imao Amazon, koji je daljinskim putem, svojim korisnicima izbrisao kopije knjiga sa njihovih Amazon Kindle čitača. Iako je usledilo izvinjenje, refundacija korisnika i objašnjenje da je do toga došlo zbog problema sa autorskim pravima kod izdavačke kompanije koja je ustupila Amazonu on line prodaju, ovaj postupak je komentaran kao "orvelijanski" (aludirajući na Orvelovu knjigu "Veliki brat"), posebno jer se i radilo o dve Orvelove knjige ("1984" i "Životinjska farma"), uz zahteve Amazonu da ukine DRM [28].

Dokumenti

Enterprise digital rights management (E-DRM ili ERM) je primena DRM tehnologije na kontrolu pristupa dokumentima organizacije, kao što su Microsoft Word, PDF i AutoCAD fajlovi, poruke elektronske pošte, intranet web stranice itd, a ne mediji sa sadržajima za krajnje korisnike. E-DRM se sve češće naziva i IRM (*Information Rights Management*), čija je osnovna namena sprečavanje neautorizovanog korišćenja organizacionih dokumenata, i koji se obično integriše sa *content management* softverom.

Digitalni vodeni žigovi

Nešto ređe korišćen DRM sistem je onaj koji koristi digitalni vodeni žig, *digital watermark*. To su zapravo podaci (o vlasniku autorskih prava, distributeru ili naručiocu –kupcu), koji su skriveno upisani u audio i video sadržaje na medije tokom proizvodnje ili distribucije, korišćenjem steganografije. Primenjen na zaštitu video sadržaja, on se sastoji od malog programskog koda, koji se šalje zajedno sa

digitalnim video signalom i koji uređaju za snimanje "govori" da je taj sadržaj zaštićen, čime se onemogućuje njegovo snimanje. Ovaj sistem zahteva medije i uređaje koji mogu da čitaju digitalni vodeni žig, ali se sreće i sa problemom legalnosti primene, jer je sud u SAD, 2005. godine presudio da FCC nema pravo da određuje šta može da radi uređaj korisnika sa digitalnim signalom, kada je on već jednom isporučen.

Vodeni žigovi mogu da se koriste kao deo DRM sistema, ali više u cilju dokazivanja prava vlasništva, nego kao sredstvo za direktno ograničenje korišćenja. Neki programi za editovanje audio i video sadržaja mogu da izbrišu ili oštete vodene žigove. Takođe, poređenjem dva posebne preuzeta, a ista audio sadržaja, moguće je na relativno jednostavan način izdvojiti vodeni žig.

Ponekad se, na primer, ime poručioaca, e-mail adresa i sl, dodaju prilikom preuzimanja određenog digitalnog sadržaja, ali ne kao vodeni žig, ugrađen u taj sadržaj, nego posebno kao MPEG standardni metapodaci (to radi Apple iTunes Store za svoje DRM zaštićene i nezaštićene verzije muzičkih i video sadržaja).

Zaštita softvera

Postoje različita mišljenja o uzrocima softverske piraterije, ali svakako treba uzeti u obzir faktore kao što su mogućnost lake zarade, lakomislenost, nepoznavanje (ili nepostojanje) zakona, a posebno neshvatanje softvera kao vredne intelektualne svojine. Prva dva faktora su prisutna u svim područjima ljudske delatnosti, pa taj rizik moraju da eliminišu sami proizvođači softvera, korišćenjem određenih zaštitnih mera, dok su poslednja dva faktora najčešće predmet akcija odgovarajućih društvenih i državnih institucija.

Na problem softverske piraterije u budućnosti će uticati sve veći broj instaliranih personalnih računara, rast broja brzih internet priljučaka, rast lokalnih softverskih tržišta, tehnologije zaštite softvera i lokalni faktori, kao što su kultura, politički uslovi, efikasnost institucija itd.

Na rasprostranjenost ovog fenomena uticale su i određene zablude, kao na primer [9]:

- kopiranje nikoga ne oštećuje
- to nije krađa, ako se ne stvara profit daljom distribucijom
- tako se smanjuju troškovi firme
- male su šanse za krivičnu odgovornost
- to svi rade, itd.

Čak i kod mnogih poslovnih ljudi, pa i vlada nekih zemalja, na softversku pirateriju se gleda kao na lak način za ulazak u novu globalnu ekonomiju, zasnovanu na novim informacionim tehnologijama.

Srbija, gde je piraterija tokom devedesetih godina bila način preživljavanja, ne samo pojedinaca, nego i države u celini, je izuzetno pogodno tlo za razvoj različitih piratskih aktivnosti. Prema proceni firme *Microsoft*, u Srbiji od 1,2 miliona kompjutera, tek svaki četvrti ima licenciran operativni sistem, a još je manje onih koji imaju legalan *MS Office* paket. Prema podacima jednog od najpoznatijih sajtova za preuzimanje piratskih filmova <http://oneclickmoviez.com>, na listi zemalja iz kojih im najviše posetilaca svraća na sajt, Srbija sa 3.565.158 poseta zauzima četvrto mesto.

Uobičajeni vid zaštite softvera je enkripcija, a korišćenje enkriptovanog softvera omogućuje posebno isporučen ključ za dekrpciju. Taj ključ može da omogući samo jednokratnu instalaciju softvera, pri čemu za sve naredne instalacije mora da se traži saglasnost, ili može da bude stalni ključ, pri čemu se obično vezuje za ID brojeve elemenata računarskog hardvera određenog računara, da softver ne bi bio instaliran na bilo kom broju računara.

Neki proizvodi koriste sisteme zaštite od neovlašćenog korišćenja bazirane na Webu. Instalacijom softvera na određeni računar, kontaktira se server za verifikaciju licenci, radi dobijanja dozvole (pristupnog ključa) za pokretanje programa. Ako je to prvi računar koji traži dozvolu za instalaciju tog softvera, server šalje odgovarajući ključ, u suprotnom odbija zahtev, pa korisnik mora da se obrati

dobavljaču za dozvolu za instalaciju na drugi računar.

Finansijski efekti, odnosno gubici koje zbog softverske piraterije trpe autori, proizvođači, prodavci, a posredno i države (zbog neplaćanja poreza), su toliki (preko 60 milijardi dolara, na svetskom nivou u 2007. godini) [29], da su DRM rešenja svoje poslednje, ali i najjače uporište našla upravo u oblasti zaštite softvera.

5. ARHITEKTURA DRM SISTEMA

Idealni DRM sistem je fleksibilan, potpuno transparentan za korisnika, a istovremeno složen softverski problem. Prva generacija DRM softvera je bila orijentisana najviše na na bezbednost i enkripciju kao način rešavanja problema nedozvoljenog kopiranja digitalnih sadržaja, dok druga generacija DRM, pored zaštite, treba da unese i elemente komercijalnih aktivnosti, praćenja i kontrole ponašanja korisnika, tako da DRM postaje "digitalno upravljanje (svim) pravima", a ne samo "upravljanje digitalnim pravima".

U projektovanju i primeni DRM sistema, uočavaju se dva osnovna pristupa. Jedan je **funkcionalni pristup**, koji na najvišem nivou definiše module (komponente) sistema, a

drugi je **informacioni pristup**, koji se bavi modeliranjem entiteta unutar DRM sistema i njihovom međusobnom povezanošću [30].

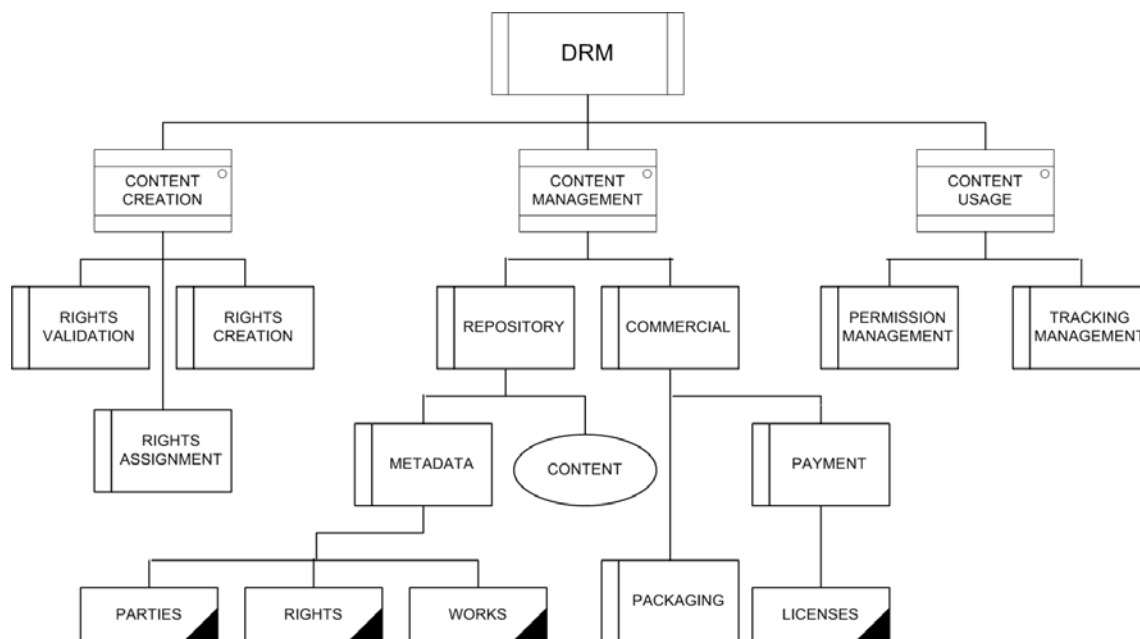
5.1. Funkcionalni pristup

Kompletan DRM sistem se može posmatrati na tri nivoa:

1. Kreiranje intelektualne svojine (digitalnog sadržaja) i definisanje vrste zaštite za određeni sadržaj,
2. Upravljanje distribucijom zaštićenog sadržaja
3. Kontrola korisnikovog korišćenja tog sadržaja.

Svaki od pomenutih nivoa se sastoji od niza međusobno povezanih modula (Slika 1). Na prvom nivou, to su:

- modul za validaciju prava – obezbeđuje da se novi sadržaj kreira na osnovu postojećeg, u skladu sa definisanim pravima
- modul za kreiranje prava – omogućuje dodelu određenih prava korišćenja novom sadržaju (prava vlasnika i prava korišćenja)
- modul za proveru i odobrenje određenih prava, za dati sadržaj.



Slika 1: Funkcionalna arhitektura DRM

Na drugom nivou, to su:

- moduli za pristup sadržajima u određenim repozitorijumima i metapodacima (*Parties, Rights, Works*)
- modul sa komercijalnim uslovima (licence, plaćanje, konfigurisanje sadržaja itd).

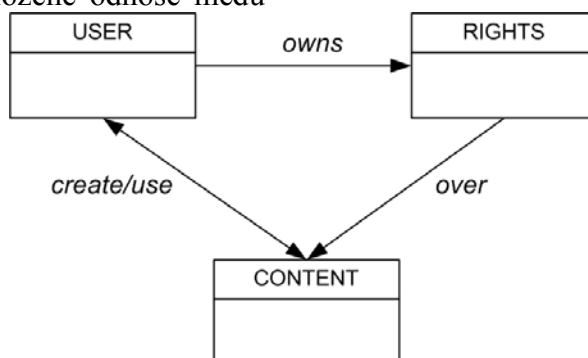
Na nivou korišćenja, koriste se:

- modul za usaglašavanje korišćenja sa pravima za određeni sadržaj (na primer, dozvoljeno je gledanje dokumenta, ali ne i štampanje)
- modul za praćenje korišćenja - kontrola da li se sadržaj koristi u skladu sa uslovima licence (na primer, dozvoljeno je 5 pokretanja određenog sadržaja). Ovaj modul mora da bude povezan sa komercijalnim modulom, ako je dogovorena naplata po korišćenju određenog sadržaja.

Moduli na sva tri nivoa moraju da obezbede i povezanost sa softverom za elektronsko poslovanje (personalizacija kupaca, potrošačke korpe itd) i softverom za upravljanje digitalnim sadržajima (ažuriranje, evidencija verzije, itd), kao i međusobnu interoperabilnost, standardni format, otvorenost i sl. [31]. Ovo zahteva i niz standardnih protokola za povezivanje tih modula, koji su još u povoju, kao što je, na primer, protokol radne grupe prodavaca elektronskih (*OpenEBook Forum's Rights & Rules Working Group for ebook vendors*).

5.2. Informacioni pristup

Funkcionalni pristup prikazuje na najopštijem nivou strukturu DRM. Složene odnose među



Slika 2: Modeliranje entiteta

modulima i njihovim entitetima treba detaljnije modelirati korišćenjem informacionog pristupa, koji obavlja tri osnovne funkcije:

- modeliranje entiteta
- identifikacija i opis entiteta
- iskazivanje (licencnih) prava.

U tom smislu, DRM program treba da dobro definiše i opiše tri osnovna entiteta – korisnik, sadržaj i korisnička prava – kao i relacije među njima.

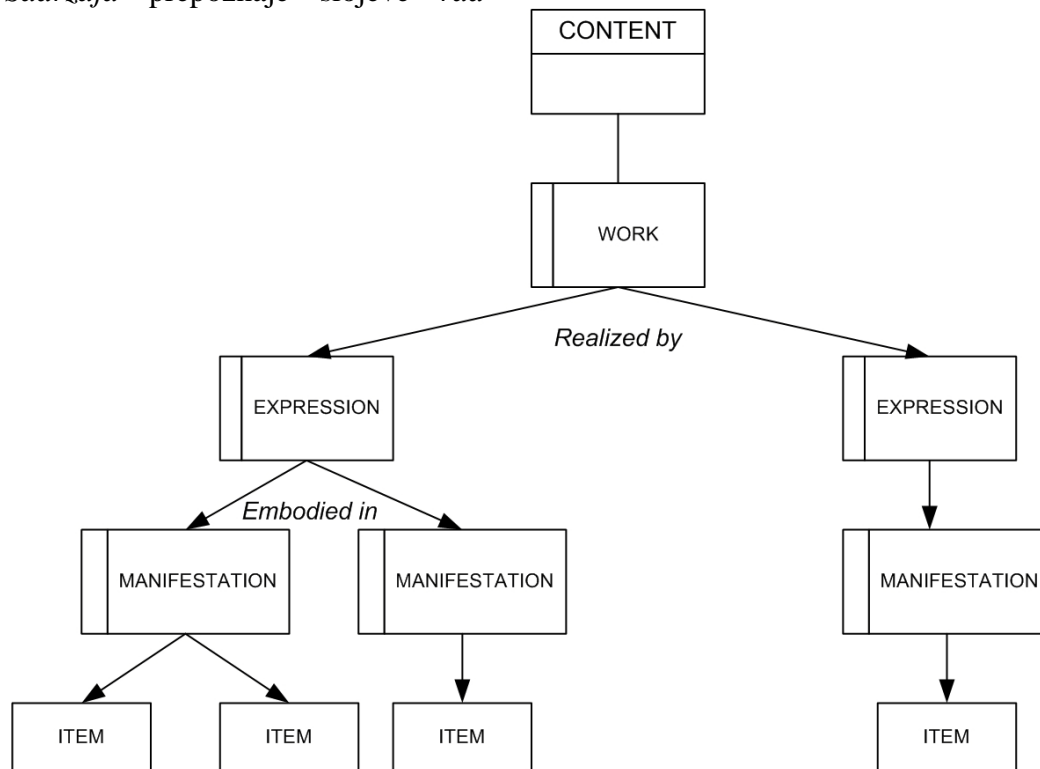
Entitet korisnika je nepromenljiv, dok sadržaj, korisnička prava, kao i odnosi korisnika sa sadržajem i pravima, mogu da se menjaju. DRM sistem mora da se brzo, tokom rada, prilagođava ovim promenama.

Modeliranje entiteta

Najčešće korišćen model je takozvani *INDECS* model (*Interoperability of data in e-commerce systems*) [32], čiji osnovni princip je jasno razgraničenje i identifikacija tri osnovna entiteta – Sadržaja, Korisnika i Prava (Slika 2). *Korisnici* mogu biti nosioci prava i krajnji korisnici. *Sadržaj* je bilo koji tip sadržaja, a entitet *Prava* govori o dozvolama, ograničenjima i obavezama između *Sadržaja* i *Korisnika*. Ovaj model omogućuje veliku fleksibilnost u dodeli prava za bilo koju kombinaciju korisnika i sadržaja i dozvoljava korišćenje sadržaja i u okviru novih poslovnih modela. Podrazumeva se da metapodaci o sva tri entiteta treba da sadrže i mehanizme za njihovo međusobno povezivanje.

Entitet *Sadržaj* takođe treba da se modelira, pri čemu se polazi od osnovnog principa da on sadrži više "slojeva", kao rezultat njegovog razvoja. Model međunarodnog bibliotekarskog udruženja (*International Federation of Library Associations – IFLA*) u okviru *Sadržaja* prepoznaje slojeve *rad*

(work), *izraz* (expression), *manifestacija* i *stavka* (item). Takav model omogućuje jasniju dodelu atributa informacijama o pravima, a na svakom sloju mogu biti podržana različita prava i nosioci tih prava (Slika 3).



Slika 3: Model entiteta *Sadržaj*

Rad (sloj sadržaja koji predstavlja jasnu intelektualnu ili umetničku kreaciju), i *izraz* (intelektualna ili umetnička realizacija rada) su kreativni oblici sadržaja. *Manifestacija* (digitalno oličenje izraza rada) i *stavka* (jedan primerak manifestacije) odražavaju fizički, ili digitalni oblik sadržaja.

U bilo kojoj tački ovog modela, moguće je uočiti različite nosioce prava, a moguć je i slučaj kada se sadržaj sastoji iz više delova, kojima su možda dodeljena različita prava, što se takođe mora uzeti u obzir.

Identifikacija i opis entiteta

Identifikacija svakog entiteta u modelu, kao i metapodataka o entitetima, treba da bude izvršena putem otvorenih i standardnih mehanizama. Otvoreni standardi, poput

Uniform Resource Identifiers (URI), *Digital Object Identifiers* (DOI) i *ISO International Standard Textual Work Code* (ISTC) su najčešće korišćeni standardi prilikom identifikacije entiteta [30].

Entitet *Sadržaj* može da se opiše nekim standardnim metapodacima za određeni žanr. Na primer, EDItEUR ONIX standard za klasične i elektronske knjige, ili IMS model (*IMS Learning Resource Meta-data Information Model*), za određene obrazovne sadržaje. Važno je da ovi standardi ne unose nove metapodatke o upravljanju pravima, jer bi to moglo da stvori zabunu. Na primer, ONIX standard sadrži elemente za definisanje broja nosilaca prava (autora i izdavača), definisanje teritorije na kojoj važe prava i jedan element za cenu, što može da predstavlja problem ako je potrebno definisati

više cena, zavisno od toga kakva prava su ugovorena.

Najpoznatiji standard za opisivanje entiteta *Korisnika* je *vCard*, koji opisuje ljude i, do određenog stepena, organizacije [33].

Lista uloga, koje može da uzima *Korisnik* u odnosu na *Sadržaj*, mogu se pronaći u tzv. MARC kodnoj listi [34].

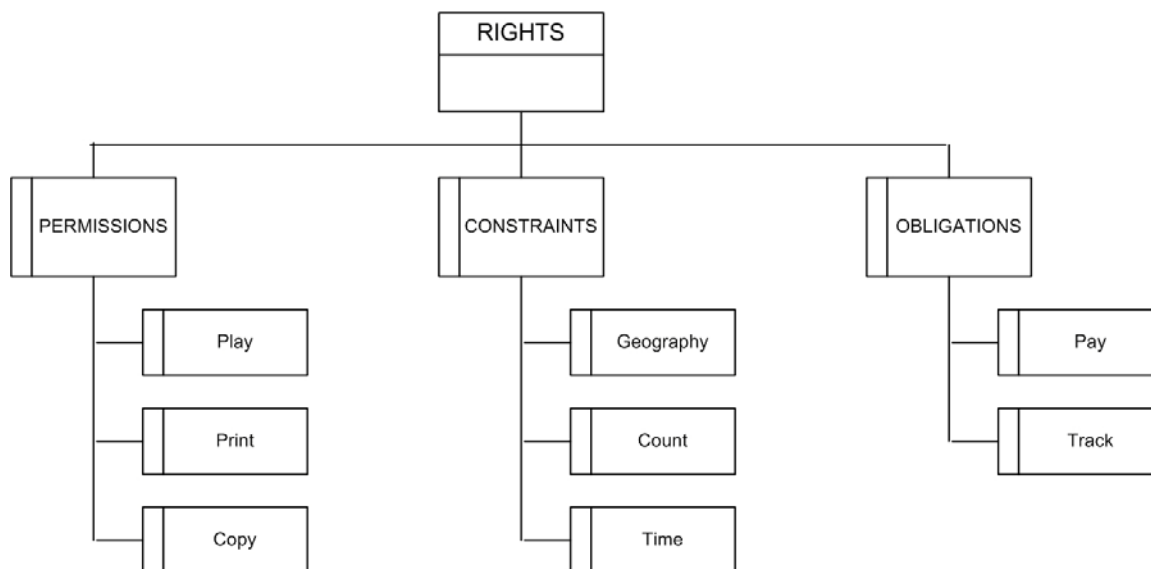
Iskazivanje prava

Entitet *Prava* omogućuje definisanje dozvola, ograničenja, obaveza i ostalih informacija o *Korisnicima* i *Sadržaju* (Slika 4). Ovi iskazi o pravima zavise od jezika koji se u tu svrhu koristi i brzo mogu da postanu veoma složeni, pa je važno i razumevanje relacija unutar ovih iskaza.

Jedan iskaz je, na primer, da određeni video sadržaj može da se pokrene (dozvola korišćenja - *permission*) maksimalno 10 puta (ograničenje - *constraint*) u prvih 6 meseci (ograničenje) po ceni od 1000,00 dinara

(obaveza - *obligation*). Svako izvođenje video sadržaja, nosiocima prava donosi određeni procenat od cene. Ukoliko korisnik želi da promeni neki od uslova korišćenja (na primer, broj pokretanja) DRM softver mora automatski da se prilagodi novim odnosima, uz uspostavljanje novih relacija unutar entiteta i među entitetima. Obično, ako pravo nije eksplicitno iskazano, znači da ono nije dodeljeno, što čini kritičnu pretpostavku jezika za opis prava koja treba da bude poznata svim Korisnicima.

Entitet *Prava* nije baš pogodan za računarsku interpretaciju, pa su razvijeni novi jezici, koji omogućuju digitalnu interpretaciju ovih iskaza. Takvi su, na primer, MPEG REL (*MPEG Right Expression Language*) i ODRL (*Open Digital, Rights Language*), računarski jezici bazirani na XML (*Extended Markup Language*), koji sadrže mnogo mogućih termina za dozvole, ograničenja, obaveze, načine plaćanja, i sl.. u različitim oblastima [35].



Slika 4: Model iskazivanja prava

6. ZAKLJUČAK

Sve navedene konverze sistema za upravljanje digitalnim pravima, ukazuju na potrebu za kreiranjem kompromisnog sistema koji bi zadovoljio i nosioce autorskih prava i

korisnike. Zbog nepostojanja standarda ili naredbi, softver za DRM se teško uklapa u postojeće arhitekture e-trgovine. Najlakši deo je kontrola preuzimanja sadržaja sa određenog sajta, a teži deo je kontrola korišćenja tog sadržaja od strane korisnika u

skladu sa ugovorenim korisničkim pravima. Njegovom standardizacijom dobio bi se sistem koji može da zaštiti digitalni sadržaj tokom njegovog celokupnog životnog ciklusa, od proizvodnje, preko distribucije do korišćenja.

DRM standardizacijom se bave mnoge organizacije, kao što su *OpenEBook Forum* (OEBF) i MPEG grupa, kada su u pitanju elektronske knjige i multimedijalni sadržaji, kao i *Internet Engineering Task Force* (IETF) i *World Wide Web Consortium* (W3C). Njihov rad, kao i rad drugih organizacija za standardizaciju je veoma važan za uspešnost DRM koncepta.

Savremena DRM rešenja, standardizacijom i otvorenim pristupom, treba da obezbede saradnju vlasnika i korisnika sadržaja, a ne da teraju vlasnike sadržaja da vrše kodiranje svojih sadržaja u nekim specifičnim formatima, ili pomoću specifičnih sistema.

DRM softver će automatski, na osnovu licencnih uslova, određivati koje su aktivnosti dozvoljene, kada je u pitanju određeni sadržaj. Najveći izazov će biti kvantifikacija, programiranje i ugradnja u licencne uslove "odgovarajućeg korišćenja", koje će računar moći da razume. To ostavlja prostor za dalja istraživanja o primeni savremenih informacionih tehnologija u ovoj oblasti.

7. LITERATURA

- [1] <http://drm.info>
- [2] http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html
- [3] <http://www.copyright.gov/legislation/dmca.pdf>
- [4] Doctorow, C. "DMCA's author says the DMCA is a failure, blames record industry". http://boingboing.net/2007/03/24/dmca_author_says_th.html. 2007.
- [5] http://europa.eu/legislation_summaries/information_society/data_protection/126053en.htm
- [6] <http://www.indicare.org/tiki-page.php?pageName=ProjectDescription>
- [7] <http://www.axmedis.org/com/>
- [8] Savic, Z., Darovitost i etički principi u sajber svetu, 17. okrugli sto, Vršac 2011.
- [9] Savic, Z., Softverska piraterija kao oblik sajber kriminala, TKR Palic, 2008.
- [10] http://w2.eff.org/IP/DMCA/Feliten_v_RIAA/
- [11] Walker, J., "The Digital Imprimatur: How big brother and big media can put the Internet genie back in the bottle". <http://www.fourmilab.ch/documents/digital-imprimatur/>. 2003.
- [12] Stallman, R., "The Right to Read". <http://www.gnu.org/philosophy/right-to-read.html>
- [13] "Bill Gates On The Future Of DRM.". <http://www.techcrunch.com/2006/12/14/bill-gates-on-the-future-of-drm/>
- [14] "Frequently Asked Questions about the GNU Licenses - GNU Project - Free Software Foundation". <http://www.fsf.org/licensing/licenses/gpl-faq.html#DRMProhibited>. 2010.
- [15] "The Campaign to Eliminate DRM". <http://www.defectivebydesign.org/>. 2010.
- [16] "FTC Town Hall to Address Digital Rights Management Technologies". <http://secure.commentworks.com/ftc-DRMtechnologies/>. 2009.
- [17] Schneier, B., "Quickest Patch Ever". <http://www.wired.com/politics/security/commentary/securitymatters/2006/09/71738>.
- [18] "Digital Rights Management (DRM) Systems and Copy Protection Schemes," <http://www.eff.org/IP/DRM>
- [19] Mori, R., Masaji, K., *Superdistribution: The Concept and the Architecture* The Transactions Of The Ieice; Vol.E 73, No.7 July 1990; <http://www.virtualschool.edu/mon/ElectronicProperty/MoriSuperdist.html>

- [20] http://en.wikipedia.org/wiki/Advanced_Access_Content_System
- [21] http://www.cablelabs.com/openable/primer/cablecard_primer.html
- [22] http://www.etsi.org/deliver/etsi_ts/102800_102899/10282504/01.01.01_60/ts_10282504v010101p.pdf
- [23] McMillan, R "Settlement Ends Sony Rootkit Case".
<http://www.pcworld.com/article/id,125838-page,1c,unresolvedtechstandards/article.html>. 2006.
- [24] Marechal, S., "DRM on audio CDs abolished".
<http://laxer.com/module/newswire/view/78008/index.html>. 2007.
- [25] http://en.wikipedia.org/wiki/E_Music
- [26] Fisher, K., "Musicload: 75% of customer service problems caused by DRM".
<http://arstechnica.com/news.ars/post/20070318-75-percent-customer-problems-caused-by-drm.html>. 2007.
- [27] Foster, E., "E-Books and DRM". Info World.
<http://www.gripe2ed.com/scoop/story/2004/2/19/0515/77045>. 2004.
- [28] Cashmore, P., "Big Brother: Amazon Remotely Deletes 1984 From Kindles".
<http://mashable.com/2009/07/17/amazon-kindle-1984/> 2009.
- [29] 2007 Piracy Study, BSA & IDC, www.bsa.org
- [30] Ianella, R., DRM Architectures, D-Lib Magazine, Vol. 7, no 6. June 2001.
- [31] Erickson, John S., "Information Objects and Rights Management" *D-Lib Magazine*, April 2001 Volume 7 Number 4
<http://www.dlib.org/dlib/april01/erickson/04erickson.html>
- [32] <http://www.indecs.org>
- [33] <http://www.ietf.org/rfc/rfc2426.txt>
- [34] <http://lcweb.loc.gov/marc/relations/re0003r2.html>
- [35] <http://odrl.net/>