Primerjava sistemov za upravljanje digitalnih pravic za organizacije

[1]Urška Lah, [2]Boštjan Brumen
[1]EMO – Orodjarna, d. o. o.
[2]Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova 17, 2000 Maribor
urska.lah@emo-orodjarna.si; bostjan.brumen@um.si

Izvleček

Sistemi za upravljanje digitalnih pravic nadzirajo uporabo digitalnih vsebin, preprečujejo anonimni oziroma vsaj nekontrolirani dostop do digitalnih vsebin, varujejo slike, avdio ali video datoteke pred prenosi, kopiranjem, shranjevanjem in tiskanjem ali dovoljujejo zgolj njihovo omejeno uporabo. V prispevku smo predstavili funkcionalnosti sistema za upravljanje digitalnih pravic. Na podlagi oblikovanih kriterijev za izbor smo ocenili izbrane sisteme za upravljanje digitalnih pravic za organizacije. Analiza je pokazala, da med njimi obstajajo razlike, za najboljša sistema pa sta se izkazala EMC IRM in RMS. Izbira sistema za upravljanje digitalnih pravic je odvisna od potencialnega uporabnika glede na pomembnost posameznega kriterija.

Ključne besede: digitalne pravice, upravljanje, DRM za organizacije, kriteriji izbora DRM.

Abstract

Comparison of a Digital Rights Management Systems for Organizations

Digital rights management systems monitor the usage of digital content, prevent anonymous or at least unauthorized access to digital content, and protect images, audio and video files from being transferred, copied, saved and printed, or merely allow their limited use. This article introduces the functionalities of a digital rights management system. Based on the defined selection criteria we have assessed the selected digital rights management systems for organizations. The analysis shows that there are vast differences between them, though EMC IRM and RMS have turned out to be the optimal choice. The selection of a digital rights management system depends on the prospective users and their preferences of individual criteria.

Key words: Digital rights, management, DRM for organizations, DRMS selection criteria.

1 IZHODIŠČE

Kopiranje sega že daleč v preteklost. Vzemimo za primer, da je nekdo zapisal določeno besedilo. To so ljudje lahko prosto kopirali. S tem mislimo na fizične stvari. Z razvojem digitalne dobe danes prihaja do kopiranja digitalnih multimedijskih vsebin (slike, video in avdio datoteke, članki, e-knjige, programska oprema), ki so na spletu dostopne vsem. Avtorjem predstavlja to že kar prepoznavno finančno škodo, saj v to vložijo svoj trud, čas in denar (Kristan, 2009). Višina finančne škode oziroma ekonomski učinki kraje, kršitev in piratstva so odvisni od ponudbe in povpraševanja po fizičnih in virtualnih izdelkih vsebin (Picard, 2004). Preglednica 1 prikazuje finančno škodo piratstva v milijardah evrov po regijah in vrsti industrije ZDA v letu 2005.

Preglednica 1: **Finančna škoda piratstva** (Siwek, 2007)

Ameriška industrija	Azija/Pacifik (milijard €)	Evropa/CIS (milijard €)	Ameriki (milijard €)	Srednji vzhod/ Afrika (milijard €)
Film	429,9	735,1	811,9	134,8
Posneta glasba	515,3	561	821,5	62,8
Poslovna programska oprema	2.520	2.237,4	1.082,3	422,5
Zabavna programska oprema	984,2	740,2	187,3	11,3
Skupaj	4.449,4	4.273,7	2.903	631,4

Leta 2005 je bilo skupaj v vseh regijah za skoraj 17 milijard dolarjev finančne škode zaradi piratstva. V Sloveniji je bila leta 2011 stopnja piratstva 46-odstotna, tržna vrednost ukradene programske opreme je znašala 37 milijonov evrov (BSA, 2012).

Prosti dostop do preteklih del pomaga določiti bogastvo prihodnjih del (Bailey Jr., 2006). Ko so pretekla dela nedostopna, razen priviligirani manjšini, so zaradi tega prihodnja dela osiromašena. Po drugi strani pa so intelektualna dela lastnina, to pa bi morali ustrezno zaščititi. Splet je bil zasnovan tako, da ena vrsta vsebine ni imela prednosti pri hitrosti dostave pred drugo, ni bilo tega, da je bilo za dostavo ene vrste vsebine treba plačati, za drugo ne, in da je bila ena vrsta vsebine blokirana (vsaj na omrežju), druga ne (Bailey Jr., 2006). V zadnjih letih je nevtralnost omrežja napadena (Bailey Jr., 2006). S tem ko shranjevanje in posredovanje umetniških stvaritev postaja vedno bolj digitalno, se področje avtorskih pravic sooča s številnimi izzivi. Sistemi za zaščito pred kopiranjem, poznani kot sistemi za upravljanje digitalnih pravic (angl. digital rights management – DRM), lahko v prvi vrsti omilijo škodo glede avtorskih pravic s tem, ko otežijo nepooblaščeno kopiranje (Liebowitz, 2002). Uporaba tehnologij DRM narašča (Bailey Jr., 2006).

Določiti pravično uporabo ni preprosto. Mnoga podjetja so sprejela skrajne ukrepe, da bi »zakrpala luknjo« digitalnih vsebin, ki se pretakajo po spletu. Pri tem so izločila vsakršno pravico potrošnika pri odločanju glede vsebine, ki jo je kupil. Novejši sistemi DRM so šli tako daleč, da so v celoti omejili uporabnika (Layton, 2006). Eden od primerov je zaščita DVD-jev, ko uporabnik teh ni mogel kopirati v družinskem kontekstu (Orlowski, 2005). Ubisoft za kupce računalniške igre Anno 2070 omejuje število namestitev omenjene igre na računalnik na tri, poleg tega vsaka menjava grafične kartice pomeni tudi novo namestitev (Pereira, 2012). Nekateri sistemi celo na nezakonit način posegajo v pravice uporabnikov. Takšen primer je Sony BMG. Izdal je CD z zaščito XCP, ki samodejno namesti na sistem t. i. rootkit, zaradi katerega je postal uporabnikov računalnik ranljiv na napade hekerjev (Mulligan & Perzanowski, 2007). Nejasno je tudi, ali lahko zaščita avtorskih pravic še naprej zagotavlja dovolj spodbude za umetniško ustvarjanje (Liebowitz, 2002). Želje po robustnih sistemih za upravljanje digitalnih pravic zato niso nič novega (LaMacchia, 2003).

Vse to nas je motiviralo, da smo se odločili za raziskavo. Na trgu namreč obstaja mnogo sistemov DRM, ki rešujejo problem nepooblaščene uporabe (Haber, Horne, Pato & Sander, 2003). Težava je, da so ti sistemi različni, in zaradi tega se pojavi vprašanje, katerega izbrati. Problem bomo rešili s pomočjo primerjave oziroma ocene štirih sistemov DRM za organizacije, ki med drugim preprečujejo kopiranje digitalnih vsebin, po vnaprej določenih kriterijih.

V nadaljevanju predstavljamo kratek pregled literature. Opišemo pojem sistem za upravljanje digitalnih pravic, njegovo tipično arhitekturo in funkcionalnosti ter vrste sistemov DRM in njihove lastnosti. V razdelku 2 predstavimo cilje prispevka. V razdelku 3 opišemo znanstvene metode, uporabljene v raziskavi. V razdelku 4 izvedemo analizo izbranih sistemov za upravljanje digitalnih pravic in predstavimo njihove prednosti in slabosti – opišemo rezultate. V razdelku 5 sklenemo naš prispevek s končnimi ugotovitvami.

Naša raziskava je povezana z delom avtorjev Arnaba in Hutchisona (2005), ki preučuje zahteve sistemov DRM za organizacije (dokumentne sisteme DRM). Našemu delu je sorodno tudi delo avtorjev Michielsa, Joosena, Verslypeja in De Deckerja (2005), ki podaja kritično oceno sistemov DRM. Avtorja Zeng in van Moorsel (2011) prav tako naredita pregled nad priljubljenimi izdelki DRM, trenutno prisotnimi na trgu, glede na njihove skupne značilnosti in razvijeta metodo, s katero lahko kvantitativno ocenimo vpliv tehnologije DRM. Sohn (2007) predstavi ključne dejavnike za oceno in primerjavo sistemov DRM. Arjona in Grenman (2005) razvijeta skupni niz kriterijev za oceno odprtih in lastniških rešitev DRM izbranih proizvajalcev, osredinjenih na zaščito digitalne glasbe.

1.1 Pojem sistem za upravljanje digitalnih pravic

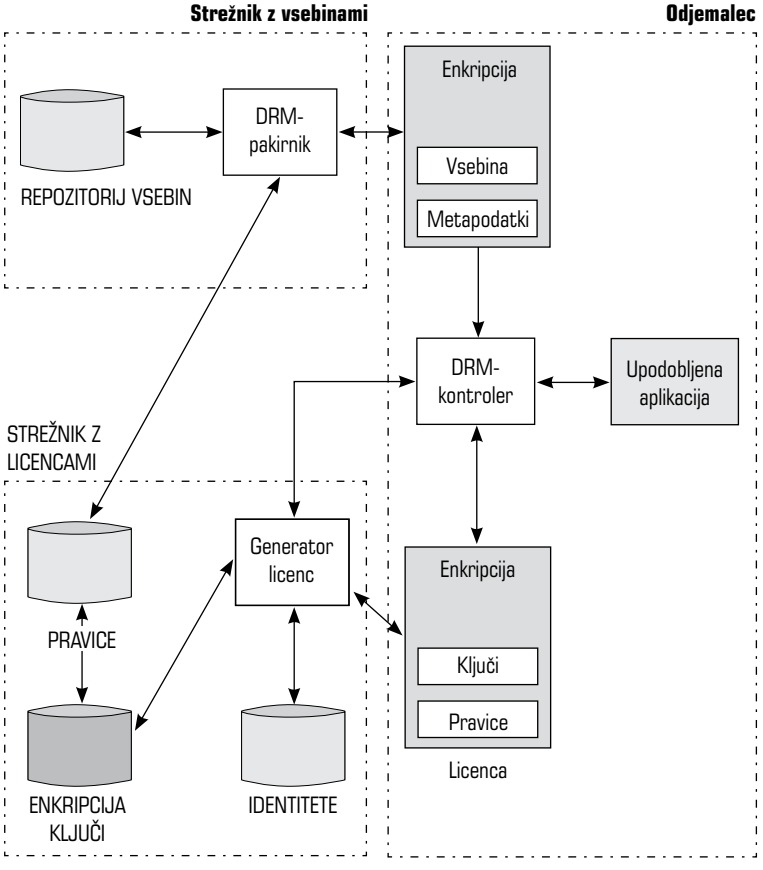
Sistemi za upravljanje digitalnih pravic (sistemi DRM) so običajno opredeljeni kot niz tehnoloških ukrepov, s katerimi imetniki pravic preprečujejo uporabo digitalnih vsebin, za katere dajejo dovoljenja, ki bi lahko ogrozila tržno vrednost njihovih izdelkov. Omejitve uporabe, kot so prenosi, tiskanje, shranjevanje in pošiljanje e-pošte, so kodirane neposredno v izdelek ali strojno opremo, potrebno za njihovo uporabo (takojšnji učinek) (Kasprowski, 2010). DRM je sklop storitev programske in strojne opreme ter tehnologije, ki ne samo da urejajo dovoljeno

uporabo digitalnih vsebin, temveč tudi upravljajo s posledicami uporabe skozi ves življenjski cikel vsebine (Duhl & Kevorkian, 2001). DRM varuje datoteke s preprečevanjem kopiranja ali da dovoljuje le omejeno uporabo (Broussard, 2007). DRM je tehnologija, ki opisuje, opredeljuje in ščiti digitalno vsebino, obenem pa je zaščitena s pravicami intelektualne lastnine skladno s pravili, določenimi od imetnikov pravic ali predpisanih z zakonom (Shukla & Chaturvedi, 2004). Pojem se nanaša na katero koli od številnih tehničnih metod, ki se uporabljajo za nadzor ali omejevanje uporabe digitalnih del, zaščitenih z avtorskimi pravicami. V določenih primerih tehnološki ukrepi zaščite rezultirajo tudi v omejenem dostopu do avtorsko zaščitenih del. Kot odgovor na skrb glede nezakonitega kopiranja in nepooblaščene distribucije digitalnih del DRM vedno pogosteje uporabljajo z vsakdanjimi potrošniškimi izdelki, kot so avdio CD-ji, DVD-ji in e-knjige. Te tehnologije se uporabljajo za opredelitev tega, za kaj želi nosilec avtorskih pravic, da se zaščiteno delo uporablja. S tem se prepreči kakršna koli nadaljnja uporaba, ki ni določena za to. Sem spadajo obseg, trajanje in drugi vidiki uporabe ter preprečitev vseh nedoločenih nepooblaščenih uporab (OECD, 2006).

Poznavalci menijo, da je DRM trenutno najbolj napreden tehnološki ukrep. Z njegovo pomočjo je mogoče nadzirati uporabo digitalnih vsebin (Kristan, 2009). Ti sistemi so za imetnike pravic zelo privlačni, saj omogočajo upravljanje avtorskih pravic neposredno z vsakim končnim uporabnikom posebej (Bogataj Jančič v Breznik, Bogataj Jančič, Kovačič & Milohnić, 2008). Poglavitni namen DRM je preprečiti anonimni oziroma vsaj nekontrolirani dostop do digitalnih vsebin (Kristan, 2009).

1.2 Arhitektura sistema DRM

Tipično arhitekturo[1] sistema DRM prikazuje slika 1.



Slika 1: **Arhitektura sistema DRM** (Yu & Chiueh, 2004)

[1] Tipično arhitekturo je sprejela večina raziskovalcev. Vključuje tri elemente: paket vsebine, strežnik z licencami in odjemalca. Deluje skladno s protokoli med omenjenimi tremi elementi.

Sistem DRM je sestavljen iz odjemalca, strežnika z vsebinami in strežnika z licencami. Odjemalec je sestavljen iz kontrolerja (za sprejem uporabnikove zahteve in komunikacijo s strežnikom z licencami) in upodobljene aplikacije (mnogo sistemov, npr. Microsoft Windows Media Rights Managment – WMRM). Strežnik z vsebinami shranjuje zaščitene datoteke v repozitoriju vsebin in pripravi paket vsebine (šifrirani metapodatki vsebine). Uporabnik sistema DRM mora pridobiti licenco, preden lahko dostopa do določenega dela vsebine. Ta vsebuje informacijo o pravicah, opredelitvi vsebine, na katero se nanašajo pravice, in identiteti uporabnika/naprave, ki želi na vsebini uveljavljati pravice. Licence generira licenčni generator. Strežnik z licencami shranjuje identitete uporabnikov (informacije o uporabnikih, ki uveljavljajo pravice za vse zaščitene vsebine) (Yu & Chiueh, 2004).

1.3 Funkcionalnosti sistema DRM

Glavni namen sistema DRM je zagotavljanje digitalne vsebine na način, ki ščiti avtorske pravice ponudnikov vsebin, in omogočanje možnosti za nove poslovne modele za distribucijo in dostop vsebin (Popescu, Crispo, Tanenbaum & Kamperman, 2004).

Nekatere pomembne značilnosti, ki naj bi jih imel učinkovit sistem DRM, so (Windley, 2005):

- stalna varnost, kjer koli obstaja digitalni vir;
- ločena pravica dostopa do informacij;
- upravljanje posameznih pravic (pogled, tiskanje, urejanje, zaslonska slika);
- dinamično dodeljevanje in odvzem pravic;
- podpora delu s povezavo in brez nje;
- revizijska sled ukrepov in aktivnosti, ki se izvajajo na dokumentu;
- podpora več oblikam dokumentov z uporabo istih varnostnih orodij;
- preprosta integracija z obstoječim potekom dela in aplikacijami;
- integracija s sistemi za upravljanje z dokumenti/vsebinami.

Popoln sistem DRM z vsemi navedenimi značilnostmi ne obstaja (Windley, 2005).

Ena od funkcionalnosti sistema DRM je, da lahko uporabnik vidi samo eno poglavje iz e-knjige, zaščitene z DRM, in tega tudi ne more natisniti (Bailey Jr., 2006).

Nadzor nad kopiranjem (angl. copy control) imenujemo sposobnost nadzora nad tem, ali uporabnik lahko dela kopijo nečesa (tiskani izvodi, računalniške kopije ali oboje). Ta nadzor je težko doseči. Preprečiti ljudem, da bi kopirali računalniške datoteke, je zelo težko, če ne celo nemogoče (Locklizard, 2013), podobno pa je z nadzorom kopiranja. Na neki stopnji nadzora kopiranja je nemogoče preprečiti nekomu, da se usede za računalnik s kamero in naredi sliko vsega, kar vidi na zaslonu. Spet na drugi stopnji se lahko zelo oteži ali naredi zelo neugodno za nekoga, ki želi narediti kopije nečesa – nima vsakdo kamere, ki je zmožna narediti dobre slike z visoko ločljivim zaslonom z namenom narediti sprejemljivo kakovostno kopijo. Lahko se sicer prepričamo, da samo pooblaščeni uporabniki ustvarjajo kopije, vendar če lahko naredijo kopijo, ki jo lahko potem uporabi kdo drug, smo ponovno na začetku. Nadzor kopiranja je torej zagotoviti orodja DRM, da kakovost kopij (kjer to dovolimo) intelektualne lastnine ni dovolj dobra, da bi to ogrozilo vrednost našega dela (Locklizard, 2013).

Sistem DRM omogoča nadzor dostopov v datoteke (angl. File Access Control) (CISCO, 2013). Nadzor dostopa ugotavlja, ali uporabnik (človek, proces, računalnik itd.) lahko izvaja operacijo (branje, pisanje, izvajanje, brisanje, iskanje itd.) nad objektom (v podatkovni bazi, tabeli, datoteki itd.) (Romuald & Coulondre, 2006). V najboljšem primeru bi morali biti vsi dostopi upravljani prek odlično razvitega sistema za nadzor dostopa, temelječega na vlogah. Posamezniki v organizacijah bi morali imeti dobro in natančno določene vloge, nadzor dostopa do vseh pa bi moral temeljiti izključno na teh vlogah. Kadar bi uporabnik spremenil svojo vlogo, bi se mu njegove pravice dostopa do vseh virov v skupni rabi samodejno spremenile glede na novo vlogo s takojšnjim učinkom (Das, Bhagwan & Naldurg, 2010). Lahko se uporabi npr. kombinacija tehnike seznama za nadzor dostopov (angl. access control list – ACL) in ključa seje (isti dokument je šifriran samo enkrat) simetričnega šifriranja (angl. encryption). To rešuje problem souporabe in delegiranja pravic dostopa za zaupne dokumente (Yiu, Yiu, Lee, Li & Yip, 2006). Pri tem lahko omejimo tudi število pogledov dokumenta ali trajanje pogledov (CISCO, 2013).

Sistem DRM zagotavlja omejitve glede spreminjanja, skupne rabe, shranjevanja in tiskanja, obenem pa tudi šifrira datoteke za uporabo samo pooblaščenim uporabnikom (CISCO, 2013). S šifriranjem vsebin onemogočimo nepooblaščene dostope do vsebin. Če se razbije algoritem šifriranja, je vsebina razkrita.

1.4 Vrste sistemov DRM in njihove lastnosti

Obstoječe sisteme DRM lahko razvrstimo v različne kategorije glede na različne standarde, npr. izbrano tehniko zaščite ali ščiteni objekt – programska oprema, e-knjiga, slike, pretočne vsebine,[2] vsebine na mobilnih napravah (Wang & Liu, 2008).

Glavna funkcija sistema DRM za zaščito programske opreme je previdnost glede piratstva programske opreme (Wang & Liu, 2008). Pri programski opremi je značilna uporaba licenc za zaščito avtorskih pravic (angl. copyright), proste licence[3] (Gehring, 2006) in »community edition« licence.

Sistemi DRM za zaščito e-knjig imajo dve vrsti aplikacij: spletne knjigarne (Amazon, eReader) in digitalne knjižnice (netLibrary, Apabi). Prve prodajajo e-knjige neposredno bralcem, druge zagotavljajo samo storitev izposoje. Obe morata ščititi pravice pred kršitvami tretjih oseb (Wang & Liu, 2008).

Sistemi DRM za zaščito slik so bolj zapleteni. Nekatere spletne strani na slike vstavijo svoj logotip. S tem drugim preprečijo njihovo nezakonito rabo. Vendar vidni logotip povzroči nižjo kakovost slike (Wang & Liu, 2008). V slike lahko vstavimo tudi nevidni vodni tisk (angl. watermark). Vodni tisk s pravicami intelektualne lastnine z določenim algoritmom vstavimo npr. v sliko. Vsebuje informacije o lastniku (Zhang, 2009).

Digitalni vodni tisk prav tako uporabljamo na trgu pretočnih medijev. Sistemi DRM za zaščito pretočnih medijev ščitijo elektronsko glasbo, filme in video posnetke (Wang & Liu, 2008). Preglednica 2 prikazuje različne sisteme DRM in njihove osnovne značilnosti.

Preglednica 2: **Različni sistemi DRM** (Wang & Liu, 2008)

Koncepti / Zaščiteni objekt	Arhitektura	Zaščita vsebine	Preverjanje pristnosti
Programska oprema	Struktura odjemalec/strežnik	Šifriranje Digitalni vodni žig	ID strojne in programske opreme
E-knjiga	Tipična struktura[4]	Šifriranje Digitalni vodni žig	Uporabnik/geslo
Pretočni mediji	Tipična struktura	Šifriranje Digitalni vodni žig	Uporabnik/geslo ID strojne opreme

2 CILJI

Namen raziskave je analiza posameznih sistemov DRM, njihova medsebojna primerjava po izbranih kriterijih in podaja ocene. Cilj raziskave je izbrati ustrezen sistem.

3 METODE

Podatke smo pridobili s pomočjo objavljenega gradiva (knjige, članki, študije, spletne strani) v knjižnicah, e-knjižnicah ter primarnih in sekundarnih znanstvenih bazah. Iz zbranih podatkov smo izluščili relevantne podatke, tj. podatke, ki se navezujejo samo na našo raziskavo. Pridobljene podatke smo primerjali po prej izbranih kriterijih. Pri izboru kriterijev smo se opirali na podobne že opravljene študije.

Uporabili smo metodo analize in sinteze. Pri analizi smo problem razdelili na čim manj povezane oziroma sklopljene in odvisne podprobleme, ki smo jih preučevali individualno. Potem smo rešitve posameznih podproblemov združili (sinteza).

S pomočjo indukcije smo sklepali od posebnega k splošnemu (poznamo lastnosti DRM-ja in na tej podlagi sklepamo o lastnostih vseh DRM-jev).

Sisteme DRM, katerih prednosti in slabosti smo ugotavljali, smo izbrali po načelu, da bi opravili pregled nad sistemi, ki ponujajo zaščito DRM za organizacije. Odpadli so sistemi DRM za programsko opremo in vsebine. To je najpomembnejših šest sistemov DRM, ki ustrezajo našemu kriteriju. Pomembnost smo ocenjevali na podlagi kriterija

[2] Glasba in video.
[3] Angl. copyleft.
[4] Tipična struktura se nanaša na sliko 1. Večina sistemov DRM je razvitih skladno s tipično arhitekturo. Primera druge strukture sta MPEG-4 in MPEG-21.

»najpomembnejši ponudniki« (tržna napoved do leta 2018 – preglednica 3).

Preglednica 3: **Najpomembnejši ponudniki sistemov DRM za organizacije** (Howarth & Reinhold, 2006)

Tip DRM	Najpomembnejši ponudniki[5]
DRM za organizacije	Adobe, Avoco Secure, EMC Corporation (Authentica), Liquid Machines, Microsoft, Sealed Media

3.1 Izbor kriterijev

Prednosti in slabosti izbranih sistemov DRM smo iskali po vnaprej določenih kriterijih: enostavnost uporabe, učinkovita orodja za upravljanje, upravljanje politike, prilagodljivost zmogljivosti (angl. scalability) in integracija z več tehnologijami, kontrola nad upravljanjem dostopov brez povezave, kontrola nad različicami dokumentov, preprečevanje tajenja (angl. non-repudiation), varni komunikacijski kanali, varstvo zajema širokega nabora naprav, kontrole varnosti (angl. security controls), revizija (angl. audit), varovanje podatkov pred izgubo in obnova po katastrofi (angl. disaster recovery) ter cena.

Enostavnost uporabe

Raziskava analitikov, ki so sodelovali s Sealed Media, je pokazala, da je za 50 odstotkov teh enostavnost uporabe za končne uporabnike največji zadržek pri splošnem sprejetju tehnologije DRM za organizacije. Večina ponudnikov trenutno dela na izboljšavah na tem področju, saj želijo premagati zaskrbljenost kupcev glede enostavnosti uporabe (Howarth & Reinhold, 2006).

Učinkovita orodja za upravljanje

Za vsakega uporabnika, ki ima lahko več sklopov pravic – morda en sklop za vsak dokument, do katerega lahko dostopa –, je učinkovito upravljanje DRM za organizacije bistvenega pomena. Morebitni kupci iščejo centralizirane zmogljivosti upravljanja, ki pokrivajo vse procese (Howarth & Reinhold, 2006).

Upravljanje politike

Pod upravljanje politike spadajo ustvarjanje novih politik, dostop na podlagi uporabnika/vloge/skupine, sprememba/prekinitev dostopa, beleženje in merjenje uporabe, kopiranje in brisanje politik, dodajanje/odstranjevanje politike administratorjev (Allen, 2011). Večina ponudnikov zagotavlja predloge skupnih politik, nameščenih v tipičnih podjetjih. Zagotavljajo tudi ustvarjanje prilagojenih politik glede na potrebe. Za lažje upravljanje lahko politike uporabimo na skupinah uporabnikov, katerih pravice so definirane glede na njihovo vlogo v organizaciji (Howarth & Reinhold, 2006).

Prilagodljivost zmogljivosti in integracija z več tehnologijami

Integracija se izkazuje v možnosti uporabe na različnih operacijskih sistemih odjemalca (Windows, Mac OS, Linux) in šifriranja, napravah (namizne, mobilne), aplikacijskih strežnikih, podprtih oblikah datotek (PDF, Excel, Word, Powerpoint, CAD) ter v tem, ali je rešitev dostopna brez integracije odjemalca (komponente, vtičniki) ali z njo (Allen, 2011). Ponudnike vsebin zanima, kako fleksibilna je tehnologija – bolj ko je fleksibilna, več nadzora bodo imeli nad vsebinami (Arjona & Grenman, 2005). Sistem DRM mora podpirati fleksibilnost v prenosu, shranjevanju in dostopu do digitalnih vsebin na različnih platformah (Ku & Chi, 2004).

Kontrola nad upravljanjem dostopov brez povezave

V današnjem izjemno mobilnem svetu je pomembno, da imajo oddaljeni uporabniki ali tisti, ki potujejo, dostop do poslovnih dokumentov, kadar nimajo povezave in tudi ko so povezani z omrežjem podjetja. Upravljanje z uporabnikovimi dovoljenji in pravicami mora biti tudi razširljivo v tem smislu, da pokrije uporabo dokumentov v načinu brez povezave in da se ne izgubi varnost. Nekateri ponudniki tehnologije zagotavljajo možnost časovne kontrole dostopa, kot je omogočanje dostopa do dokumentov za tri dni, preden je uporabnik prisiljen povezati se v omrežje podjetja za posodobitev dovoljenj, povezanih s tem dokumentom, ali za zagotovitev, da uporabljajo zadnjo različico dokumenta. Sem spadajo še zmožnost preklica pravic, kot je dostop do dokumenta ali dinamične kontrole nad pravicami, kot je izklop možnosti tiskanja dokumenta, ne da bi moral biti uporabnik povezan, da bodo začela veljati nova dovoljenja (Howarth & Reinhold, 2006).

[5] Sealed Media produkt Enterprise DRM je prevzel Oracle. Produkt se sedaj imenuje Oracle IRM (Thorpe, 2008). Ta sistem ni več v prodaji, zato smo ga izvzeli iz raziskave. DRM od Avoco Secure (secure 2 Trust) trenutno razvijajo za oblak, zato ni na voljo in smo ga prav tako izvzeli iz raziskave.

Kontrola nad različicami dokumentov

Da bi dosegli, da bodo vsi uporabniki delali na zadnji različici dokumenta in ne na zastareli različici, zmogljivosti dinamične kontrole nad različicami v DRM zagotavljajo, da so na voljo zadnje posodobljene različice tistim, ki delajo zunaj omrežja podjetja, kot tudi znotraj njega. Tehnologije DRM za organizacije omogočajo uporabnikom ali upravljavcem dokumentov spremembe politik uporabe, povezanih s točno določenim dokumentom, tako da prekličemo dostop do starejših različic dokumenta. V večini sistemov DRM so uporabniki preusmerjeni na povezavo do novega posodobljenega dokumenta, ne glede na to, kje je dokument trenutno shranjen v omrežju (Howarth & Reinhold, 2006).

Preprečevanje tajenja

Z namenom, da bi zagotovili popolnost revizijskih kontrol, morajo tehnologije DRM zagotoviti možnost označevanja dokumentov z žigom (datum, čas in ime), da nihče ne more zanikati določene akcije opravljene nad dokumentom (Howarth & Reinhold, 2006). Digitalni podpis služi kot dokaz pri predstavitvi tretji osebi, da je podpis pristen, resničen in verodostojen, kar imenujemo preprečevanje tajenja (Smallwood, 2012).

Varni komunikacijski kanali

Omogočeno mora biti varno posredovanje DRM-zaščitene vsebine prek javnih kanalov (svetovni splet, brezžična omrežja) brez tveganja prestrezanja. Informacije o uporabi dokumentov, zbrane prek sistema DRM, lahko zahtevajo zaščito v prehodu/prenosu (angl. transit) zaradi vprašanj glede zasebnosti in komercialnih interesov (Howarth & Reinhold, 2006). Preverjanje pristnosti se lahko izvede na strani uporabnika, računalnika, domene, prek pametne kartice ali piškotkov (Allen, 2011).

Varstvo zajema širok nabor naprav

Zaposleni vse bolj delajo z oddaljene lokacije ali od doma, pri tem pa uporabljajo različne naprave (prenosni računalnik, mobilni telefon, dlančnik) za dostop do poslovnih informacij. Stranke z razpršenim poslovanjem ali z veliko mobilne delovne sile bi morale razmišljati o DRM za organizacije, ki vključujejo podporo za širok nabor računalniških platform in naprav (Howarth & Reinhold, 2006).

Kontrole varnosti

Varnost je področje, nad katerim so ponudniki vsebin najbolj zaskrbljeni (Arjona & Grenman, 2005). Varnost zagotavljata raven šifriranja in upravljanje s ključi (Allen, 2011). Zmogljivost šifriranja je glavna kontrola varnosti, ki bi jo bilo treba zagotoviti v katerem koli sistemu DRM. Medtem ko ni treba, da so vse informacije šifrirane, si podjetja morda bolj želijo ustvariti in uveljaviti politike, kot je šifriranje zelo občutljivih informacij glede na njihovo klasifikacijo, kot pa prepustiti končnemu uporabniku odločitev o tem, ali komunikacijo šifrirati ali ne. Večina tehnologij prav tako zagotavlja zmožnost, da uporabniki šifrirajo dokumente po želji. Podjetja bi morala pri tem iskati dobre zmožnosti upravljanja s potrdili (angl. certificate) in digitalnim podpisom (angl. digital signature) in gledati tudi na enostavnost uporabe. Za višjo raven varnega dostopa je treba razmišljati o varnostnih žetonih (angl. token) ali biometriji (Howarth & Reinhold, 2006). Obstaja več meril za oceno varnosti sistemov DRM, npr. okvare posamezne točke (angl. single point of failure) in možnost posodobitve (delov) sistema (Jonker, Mauw, Verschuren & Schoonen, 2004).

Revizija

Z namenom dokazati, da so informacije ohranile svojo integriteto in raven zaupnosti, potrebno glede na pravice in niz dovoljenj, je bistvenega pomena, da tehnologije DRM za organizacije vključujejo močno revizijsko zmogljivost. Vse opravljene akcije se morajo zapisati na centralni lokaciji, z akcijami, vezanimi na identitete uporabnikov (polna odgovornost), zapisi pa morajo biti na voljo za potrebe analiz vodstva, ki jih lahko preuči (Howarth & Reinhold, 2006).

Varovanje podatkov pred izgubo (angl. backup) in obnova po katastrofi (angl. disaster recovery)

Sistem DRM mora biti združljiv z varovanjem poslovnih podatkov pred izgubo in načrti za obnovo po katastrofi. Zmožnosti in žetoni, potrebni za upravljanje, morajo biti na voljo na nadomestni lokaciji. Lahko da bo treba hitro prilagoditi vloge in dovoljenja med postopkom obnovitve. Poskrbljeno mora biti tudi za ureditev hrambe ključev in žetonov DRM v primeru, da zaposleni, ki običajno upravljajo sistem, postanejo nezmožni za to ali zapustijo podjetje v sovražnih pogojih (Howarth & Reinhold, 2006).

Cena

Upoštevati je treba ceno sistema DRM. Nepreudarno bi bilo uporabiti tehnologijo z visoko ravnjo varnosti za zaščito vsebin s sorazmerno nižjo vrednostjo ali uporabiti tehnologijo, ki zagotavlja nizko varnost, za vsebine zelo velike vrednosti (Rump, 2003).

4 REZULTATI

Z vsemi kriteriji smo v nadaljevanju ocenili vsakega od izbranih sistemov. Izbrali smo točkovno lestvico, ki smo jo priredili po delu avtorjev Arnab & Hutchison (2005):

0: Ta kriterij sploh ni izpolnjen.
1: Ta kriterij je slabo izpolnjen.
2: Ta kriterij je dobro izpolnjen, vendar se lahko še izboljša.
3: Ta kriterij je v celoti izpolnjen.

Za kriterij cena smo oblikovali lestvico:

0: Cena je zelo visoka (300 EUR ali več na uporabnika/prejemnika/licenco).
1: Cena je srednja (150–299 EUR).
2: Cena je sprejemljiva (pod 150 EUR).
3: Sistem DRM je brezplačen (angl. freeware) oziroma odprtokoden (angl. opensource).

Za vsakega od štirih sistemov DRM za organizacije navajamo, zakaj pri posameznem kriteriju niso dosegli maksimalnega števila točk.

4.1 Adobe

Adobe ponuja niz strežniških produktov DRM za podjetja. Njihov namen je upravljanje in spremljanje ključnih poslovnih elektronskih dokumentov znotraj in zunaj omrežja podjetja (Howarth & Reinhold, 2006). Obravnavani sistem je Adobe LiveCycle Rights Management.

Enostavnost uporabe: Tretje točke ni prejel zaradi časa, potrebnega, da se privadimo na uporabo – ni nobenih navodil za uporabo uporabniškega vmesnika. Različne verzije Adobe vplivajo na povezavo/uporabo produkta. Ne prikazuje seznama dovoljenj, zato uporabnik težko odpravlja težave.

Učinkovita orodja za upravljanje: Tretje točke ni prejel zaradi pomanjkanja zrnatosti dovoljenj (angl. granular permission) – osnovnih pravic. Z vidika upravljanja aplikacije je delo z dodatnimi vtičniki (angl. plug-in) v Office zelo zapleteno in zahtevno glede cen, saj veliko ključnih lastnosti zahteva Adobe Suite in ne samo bralnika Adobe.

Prilagodljivost zmogljivosti in integracija z več tehnologijami: Tretje točke ni prejel, ker sicer ima aplikacijske programske vmesnike (angl. application programming interface – API), vendar morajo partnerji zanje dodatno plačati Adobe. Poleg tega ni splošne sprejetosti integracije z drugimi rešitvami v aplikacijah odjemalca/strežnika.

Kontrola nad različicami dokumentov: Tretje točke ni prejel, ker sicer ne omogoča verzioniziranja dokumentov, temveč dovoljuje umik dokumenta po določenem času in izdajo nove povezave do zadnje različice dokumenta.

Preprečevanje tajenja: Dveh točk ni prejel, ker bi se to moralo urediti večinoma prek revizije dogodkov ali priporočljive uporabe drugega produkta, npr. Digital Signatures. Pomanjkanje podpore za e-pošto zmanjša boljše skupne scenarije za npr. Secure/Multipurpose Internet Mail Extensions – S/MIME in Information Rights Management – IRM.

Varni komunikacijski kanali: Dveh točk ni prejel, ker sistem ni namenjen varovanju komunikacijskih kanalov, ampak zaščiti dokumentov. Ker sistem gostuje na aplikacijskem strežniku, lahko omejimo dostop do sistema ali gostujočih dokumentov s tem, da omogočimo zgolj šifrirano (angl. Secure Socket Layer – SSL) povezavo do zahtev aplikacijskega strežnika.

Varstvo zajema širok nabor naprav: Tretje točke ni prejel predvsem zaradi nekaterih sprememb pri Apple za iOS 7.

Varovanje podatkov pred izgubo in obnova po katastrofi: Tretje točke ni prejel, ker je sicer obnova po katastrofi mogoča (sistem je nameščen na aplikacijskem strežniku in ima podatkovno bazo), vendar je za to treba samostojno namestiti orodja za podvajanje podatkov. Obstajajo kritične točke odpovedi (angl. single point of failure) pri povezavi z aktivnim imenikom (angl. active directory – AD) – lahko se poveže le z enim AD, kar je precej tvegano. Prav tako je odvisen od sinhronizacijskega procesa, kar ni transparentna integracija z AD.

4.2 EMC Corporation (Authentica)

EMC ponuja produkte DRM (EMC Documentum Information Rights Management – IRM) za podjetja, kar izhaja iz njegovega prevzema Authentica. Authentica je trdila, da je imela pred tem 250 strank po vsem svetu (Howarth & Reinhold, 2006).

Preprečevanje tajenja: Tretje točke ni prejel, ker za digitalni podpis obstaja možnost dodajanja dodatkov.

Varovanje podatkov pred izgubo in obnova po katastrofi: Tretje točke ni prejel, ker sicer možnost varovanja obstaja, vendar ne v tem paketu – treba je, odvisno od konfiguracije, dodati varovanje podatkov.

Cena: Dveh točk ni prejel, ker je cena trajne licence 158,23 evra na uporabnika (vzdrževanje ni vključeno).

4.3 Check Point (Liquid Machines)

Liquid Machines je prevzel Check Point in sistem se sedaj imenuje Document Security.

Upravljanje politike: Tretje točke ni prejel, ker temelji na spletu (oblak) in bodo možnosti upravljanja na mestu uporabe (angl. on-premises management) na voljo kasneje v letu 2014.

Prilagodljivost zmogljivosti in integracija z več tehnologijami: Tretje točke ni prejel, ker integracija z Microsoft Outlook Address Book ni podprta za Office 2003, omogoča pregled na mobilnih naprav le z nameščenim iOS.

Kontrola nad upravljanjem dostopov brez povezave: Tretje točke ni prejel, ker trenutno ni možnosti preprečitve dostopa, kadar uporabnik nima povezave, vendar pa se izvajajo pravilna dovoljenja.

Kontrola nad različicami dokumentov: Prejel ni nobene točke, ker ne omogoča tega.

Cena: Tretje točke ni prejel, ker sistem ni brezplačen (35,56 evra na leto na uporabnika brez popusta).

4.4 Microsoft

Microsoft razvija DRM za podjetja od leta 2001. Sprva je ponudil Windows Media Rights Management za avdio in video ter Digital Asset Server za e-knjige. Windows RMS se osredinja predvsem na zaščito Microsoft Office in formatov HTML (Howarth & Reinhold, 2006).

Kontrola nad različicami dokumentov: Tretje točke ni prejel, ker to ni rešitev za upravljanje dokumentov, ampak rešitev za zaščito informacij (ni prijazna do uporabnika, manjkajo določene napredne zmogljivosti). Zaradi povezave s Share Point lahko sicer uporabniki uporabljajo različice .doc iz Share Point ali iz Office za zagotavljanje kontrole nad različicami .doc.

Preprečevanje tajenja: Tretje točke ni prejel, ker sistem sicer uporablja digitalne podpise na dokumentih, ki so zaščiteni, vse transakcije so podpisane od strežnika, vendar pa uporabniki ne morejo dostopati do zasebnih ključev ali jih izvoziti.

Revizija: Dveh točk ni prejel, ker sistem omogoča le sledenje uporabnika, ko ta poskuša odpreti zaščiten dokument, kadar ima povezavo.

Cena: Tretje točke ni prejel, ker sistem ni brezplačen – osnovne cene so okrog 1,45 evra na uporabnika na mesec za oblačno storitev in 21,77 evra za samostojno licenco za produkt na mestu uporabe (angl. on-premises product) brez popusta. Oblačna storitev

Preglednica 4: **Rezultati ocene sistemov DRM**

Kriterij	Adobe	EMC Corporation (Authentica)	Check Point (Liquid Machines)	Microsoft
Enostavnost uporabe	2	3	3	3
Učinkovita orodja za upravljanje	2	3	3	3
Upravljanje politike	3	3	2	3
Prilagodljivost zmogljivosti in integracija z več tehnologijami	2	3	2	3
Kontrola nad upravljanjem dostopov brez povezave	3	3	2	3
Kontrola nad različicami dokumentov	2	2	0	2
Preprečevanje tajenja	1	2	3	2
Varni komunikacijski kanali	1	3	3	3
Varstvo zajema širok nabor naprav	2	3	3	3
Kontrole varnosti	3	3	3	3
Revizija	3	3	3	1
Varovanje podatkov pred izgubo in obnova po katastrofi	2	2	3	3
Cena	N/A[6]	1	2	2
Skupaj (od 39)	26	34	32	34

[6] Ni podatka – cene za Live Cycle ES niso objavljene. Znano je, da prodajno osebje sklepa pogodbe po dogovoru s stranko glede na specifične zahteve stranke. Ceno določijo prek upravitelja računa, ki je odgovoren za naš račun.

za uporabnike, ki samo uporabljajo vsebine, je brezplačna, zunanji uporabniki so prav tako brezplačni.

Rezultate ocene sistemov DRM prikazuje preglednica 4.

Kot lahko razberemo iz preglednice 4, je kriterij enostavnost uporabe v celoti pokrit pri vseh sistemih, pomanjkljivost ima samo Adobe. Učinkovita orodja za upravljanje so ustrezna pri vseh sistemih, razen pri Adobe. Upravljanje politike je zelo dobro urejeno pri vseh sistemih, razen pri Check Point. Kriterij prilagodljivost zmogljivosti in integracija z več tehnologijami je v celoti pokrit pri vseh sistemih, samo pri Adobe in Check Point najdemo pomanjkljivost. Kontrolo nad upravljanjem dostopov brez povezave v celoti pokrivajo vsi sistemi, samo Check Point malce zaostaja. Pri kontroli nad različicami dokumentov imajo vsi sistemi pomanjkljivost, Check Point tega ne omogoča. Preprečevanje tajenja v celoti omogoča Check Point, ostali sistemi imajo pomanjkljivost, Adobe vidno zaostaja. Vsi sistemi omogočajo varne komunikacijske kanale, le Adobe vidno zaostaja. Varstvo zajema širok nabor naprav pri vseh sistemih, razen Adobe ima pomanjkljivost. Vsi sistemi omogočajo kontrole varnosti. Revizijo omogočajo vsi sistemi, razen Microsofta, ki vidno zaostaja. Check Point in Microsoft v celoti omogočata varovanje podatkov pred izgubo in obnovo po katastrofi, Adobe in EMC imata pomanjkljivost. Cenovno sta ugodna Check Point in Microsoft. Naj poudarimo, da je razlika od 32 do 34 točk oziroma celo od 26 do 34 točk ekstremno majhna in je lahko posledica tudi osebnega pogleda avtorjev.

5 SKLEP

Danes na trgu obstajajo različni sistemi DRM, ki se uporabljajo za nadzor nad uporabo digitalnih vsebin, preprečujejo nepooblaščeni dostop do različnih digitalnih vsebin in ščitijo njihov prenos, shranjevanje, kopiranje in tiskanje ali omejujejo njihovo uporabo. Določeni sistemi so namenjeni samo eni vrsti vsebin, drugi podpirajo kombinacijo več vrst vsebin. Pred nakupom se je zato treba vprašati, kateri od teh sistemov bo najbolj ugodil zahtevam bodočega uporabnika. S prispevkom smo ocenili štiri izbrane sisteme DRM za organizacije na podlagi trinajstih kriterijev. Pri tem smo oblikovali metriko za ocenjevanje izbranih sistemov DRM, izbrali štiri najpomembnejše sisteme DRM za organizacije in na njih uporabili to metodo. Na podlagi izbrane metrike smo ugotovili, da sta se najbolje odrezala sistema EMC IRM in RMS. Sledi sistem Document Security in na koncu sistem LiveCycle Rights Management. Pri kriteriju kontrola nad različicami dokumentov je oceno 0 dobil Document Security. Ocenjujemo, da sta na podlagi izbranih kriterijev in metode ocenjevanja najboljša sistema EMC IRM in RMS. Končno odločitev sprejme potencialni uporabnik glede na pomembnost posameznega kriterija (npr. cena ali upravljanje politike).

Uporabljene kratice

AD – Active Directory
API – Application Programming Interface
CIS – Commonwealth of Independent States
DRM – Digital Rights Management
IRM – Information Rights Management
ODRL – Open Digital Rights Language
S/MIME – Secure/Multipurpose Internet Mail Extensions
SaaS – Software as a Service
SAML – Security Assertion Markup Language
SSL – Secure Socket Layer
XCP – Extended Copy Protection

VIRI IN LITERATURA

[1] Allen, Kristin. *Should you migrate from Adobe LiveCycle ES to FileOpen DRM?. FileOpen Systems*. Dostopno na http://www.fileopen.com/blog/bid/72603/should-you-migrate-from-adobe-livecycle-es-to-fileopen-drm (WebCite® http://www.webcitation.org/6Jckhq7z0). (14. 9. 2013).

[2] Arjona Andres, Thomas Grenman. *Evaluation Criteria for Digital Rights Management Schemes with Focus on Music E-business*. Prispevek predstavljen na Proceedings of the 12th European Conference on IT Evaluation (ECITE 2005), Turku, Finska, 29.–30. september 2005.

[3] Arnab, Alapan, in Andrew Hutchison. *Requirement analysis of enterprise DRM systems*. Prispevek predstavljen na Proceedings of the ISSA 2005 New Knowledge Today Conference, Sandton, Južna Afrika, 29. 6. – 1. 7. 2005.

[4] Bailey Jr., Charles W. Strong Copyright + DRM + Weak Net Neutrality = Digital Dystopia?. *American Journal of Sociology* 25 (2006): 116–139. Dostopno na doi:10.6017/ital.v25i3.3344 (14. 7. 2013).

[5] Breznik, Maja, Maja Bogataj Jančič, Matej Kovačič, Aldo Milohnić (2008). *Upravljanje avtorskih in sorodnih pravic v digitalnem okolju* (končno poročilo raziskovalno-razvojnega projekta Cilji raziskovalnega programa Konkurenčnost Slovenije 2006–2013). Ljubljana: Mirovni inštitut.

[6] Broussard, Sharee L. The Copyleft Movement: Creative Commons Licensing. *Communication Research Trends* 26 (2007): 3–40.

[7] BSA. 58 odstotkov uporabnikov računalnikov v Srednji in Vzhodni Evropi priznava uporabo piratske programske opreme. Tržna vrednost ukradene programske opreme v Sloveniji je lani znašala 37 milijonov evrov. Dostopno na http://globalstudy.bsa.org/2011/downloads/press/pr_slovenia_sl.pdf (WebCite® http://www.webcitation.org/6OVVt4a1c). (15. 5. 2012).

[8] CISCO. Intellectual Property Rights. CISCO. Dostopno na http://www.cisco.com/web/about/gov/issues/ip_rights.html (Archived by WebCite® at http://www.webcitation.org/6JcopfqBP). (14. 9. 2013).

[9] Das, Tathagata, Ranjita Bhagwan, in Prasad Naldurg. *Baaz: a system for detecting access control misconfigurations*. Prispevek predstavljen na USENIX Security'10 Proceedings of the 19th USENIX conference on Security, CA, ZDA, 11.–13. 8. 2010.

[10] Duhl, Joshua; Kevorkian, Susan. *Understanding DRM Systems*. IDC. 2013-09-14. Dostopno na http://www.documentmanagement365.com/Content/Exhibition6/Files/3bfdecf4-f4d0-45e2-af3b-b439f7c6101d/CM365%20-%20White%20Paper%20-%20IDC%20-%20Understanding%20Digital%20Rights%20Management%20Systems%20White%20Paper%20opt.pdf (WebCite® http://www.webcitation.org/6Jcp9dMul). (14. 9. 2013).

[11] Gehring, Robert A. The institutionalization of Open Source. *Poiesis & Praxis* 4 (2006): 54–73.

[12] Haber, Stuart, Bill Horne, Joe Pato, Tomas Sander, in Robert Endre Tarjan. If Piracy Is the Problem, Is DRM the Answer? *Lecture Notes in Computer Science* 2770 (2003): 224–233.

[13] Howarth, Fran, in Reinhold Arnold (2006). *The Exploding Market for Digital Rights Management* (Hurwitz report). Waltham, MA: Hurwitz & Associates.

[14] Jonker, Hugo L., Sjouke Mauw, Jan H. S. Verschuren, in A. T. S. C. Schoonen. *Security aspects of DRM systems*. Prispevek predstavljen na 25th Symposium on information theory in the Benelux, Rolduc, Kerkrade, Nizozemska, 2. –4. 6. 2004.

[15] Kasprowski, Rafal. Perspectives on DRM: Between digital rights management and digital restrictions management. *Bulletin of the American Society for Information Science & Technology* 36 (2010): 49–54. Dostopno na doi: 10.1002/bult.2010.1720360313 (12. 6. 2013).

[16] Kristan, Sabina. *Avtorske pravice v digitalni dobi*. Prispevek predstavljen na 6. študentski konferenci Fakultete za management Koper, Koper – Celje – Škofja Loka, Slovenija, 18.–20. 11. 2009.

[17] Ku, William, in Chi-Hung Chi. Survey on the technological aspects of Digital Rights Management. *Lecture Notes in Computer Science* 3225 (2004): 391–403.

[18] LaMacchia, Brian A. Key Challenges in DRM: An Industry Perspective. *Lecture Notes in Computer Science* 2696 (2003): 51–60.

[19] Layton, Julia. How Digital Rights Management Works. HowStuffWorks, Inc. Dostopno na http://computer.howstuffworks.com/drm.htm (WebCite® http://www.webcitation.org/6JcpsXekF). (14. 9. 2013).

[20] Liebowitz, Stan. Policing Pirates in the Networked Age. Cato Institute. Dostopno na http://object.cato.org/sites/cato.org/files/pubs/pdf/pa438.pdf. (WebCite® http://www.webcitation.org/6Jcq470Un). (14. 9. 2013).

[21] LockLizard. Copy Control. LockLizard. Dostopno na http://www.locklizard.com/copy-control.htm (WebCite® http://www.webcitation.org/6JcqAlSXd). (14. 9. 2013).

[22] Michiels, Sam, Kristof Verslype, Wouter Joosen, in Bart De Decker. *Towards a software architecture for DRM*. Prispevek predstavljen na DRM '05 Proceedings of the 5th ACM workshop on Digital rights management, VA, ZDA, 7.–10. 11. 2005.

[23] Mulligan, Deirdre K., in Aaron Perzanowski. The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident. *Berkeley Technology Law Journal* 22 (2007): 1157–1232.

[24] OECD. *Report on disclosure issues related to the use of copy control and digital rights management technologies*. OECD. Dostopno na http://www.oecd.org/internet/consumer/36546422.pdf (WebCite® http://www.webcitation.org/6JcqcGaLg). (14. 9. 2013).

[25] Orlowski, Andrew. *French court bans DVD DRM. The Register*. Dostopno na http://www.theregister.co.uk/2005/04/26/french_drm_non (WebCite® http://www.webcitation.org/6JcqktygR). (14. 9. 2013).

[26] Pereira, Chris. OP-ED: Has Ubisoft's DRM Gone Too Far? 1up.com. 2013–09–14. URL:http://www.1up.com/news/ubisoft-drm-gone-too-far. Accessed: 2013–09–14. (Archived by WebCite® at http://www.webcitation.org/6JcqsDGIY). (14. 9. 2013).

[27] Picard, Robert G. A Note on Economic Losses Due to Theft, Infringement, and Piracy of Protected Works. *Journal of media economics* 17 (2004): 207–217.

[28] Popescu, Bogdan C., Bruno Crispo, Andrew S. Tanenbaum, in Frank L. A. J. Kamperman. *A DRM security architecture for home networks*. Prispevek predstavljen na DRM '04 Proceedings of the 4th ACM workshop on Digital rights management, NY, ZDA, 25.–29. 10. 2004.

[29] Romuald, Thion, in Stéphane Coulondre. Integration of Access Control in Information Systems: From Role Engineering to Implementation. *Informatica* 30 (2006): 87–95.

[30] Rump, Niels. Definition, Aspects, and Overview. *Lecture Notes in Computer Science* 2770 (2003): 3–15.

[31] Shukla, Vishnu Kant, in Neha Chaturvedi. *DRM : Technological Measure for Digital Contents on the Silicon Plaform*. Prispevek predstavljen na 2nd International CALIBER-2004, Ahmedabad, New Delhi, 11.–13. 2. 2004.

[32] Siwek, Stephen E. *The True Cost of Copyright Industry Piracy to the U.S. Economy. IPI*. Dostopno na http://www.ipi.org/ipi_issues/detail/the-true-cost-of-copyright-industry-piracy-to-the-us-economy (WebCite® http://www.webcitation.org/6Jcr1bKe8). (14. 9. 2013).

[33] Smallwood, Robert F. *Safeguarding Critical E-Documents. Implementing a Program for Securing Confidential Information Assets*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2012.

[34] Sohn, David. Understanding DRM. *Queue – Power Management* 5 (2007): 32–39.

[35] Thorpe, Simon. *Where is Enterprise Digital Rights Management Going?*. Oracle. Dostopno na https://blogs.oracle.com/irm/entry/where_is_enterprise_digital_ri (WebCite® http://www.webcitation.org/6MgwACRQj). (17. 1. 2014).

[36] Wang, Shujuan, in Qingtang Liu. ERDRM: A Digital Rights Management System Model for Educational Resources. *Lecture Notes in Computer Science* 5145 (2008): 69–78.

[37] Windley, Phil. *Digital identity.* CA USA: O'Reilly Media, Inc., 2005.

[38] Yiu, S. M., S. W. Yiu, L. K. Lee, Eric K. Y. Li, in Michael C. L. Yip. Sharing and access right delegation for confidential documents: A practical solution. *Information & Management* 43 (2006): 607–616.

[39] Yu, Yang, in Tzi-cker Chiueh (2004). *Enterprise Digital Rights Management: Solutions against Information Theft by Insiders* (Research proficiency examination (RPE) report TR-169). New York: Department computer Scince, Stony Brook University.

[40] Zeng, Wen, in Aad van Moorsel. Quantitative Evaluation of Enterprise DRM Technology. *Electronic Notes in Theoretical Computer Science* 275 (2011): 1–174.

[41] Zhang, Yanqun. Digital Watermarking Technology: A Review. Prispevek predstavljen na FCC '09. International Conference on Future Computer and Communication, Wuhan, China, 6.–7. 6. 2009.

▪

Urška Lah je mlada raziskovalka v podjetju EMO – Orodjarna, d. o. o. Diplomirala je leta 2009. Njena raziskovalna področja zajemajo informacijsko varnost, varovanje intelektualne lastnine in revizijo informacijskih sistemov.

▪

Boštjan Brumen na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru predava predmete s področja podatkovnih baz, obdelave podatkov ter varnosti in zaščite podatkov. Raziskovalno se ukvarja z metodami inteligentne obdelave podatkov, podatkovnim rudarjenjem ter zasebnostjo in varnostjo podatkov, predvsem medicinskih. Objavil je več znanstvenih člankov s teh področij v revijah s faktorjem vpliva, med drugim tudi v vodilni reviji s področja medicinske informatike.