

Műhely

Az Országos Tudományos Diákköri Konferencia
díjnyertes pályaművei (1. rész)



Az e-könyves DRM-technológiák biztonságosságának vizsgálata

NAGY Andor

2015 áprilisában lezajlott az Országos Tudományos Diákköri Konferencia (OTDK) debreceni fordulója, melyen a két könyvtártudományi zsűri sok tehetséges hallgató közül választotta ki a díjazottakat. Két első helyezett lett: Csordás Mónika (SZTE-JGYPK) témájánál fogva a Könyv és Nevelés különdíját kapta, Jávorka Brigitta (PTE) pedig az MKE különdíját érdemelte ki. Négy hallgató részesült a Könyvtári Figyelő publikációs díjában: a pályamunkák cikkesített változatát a szerkesztőség folyamatosan bemutatja a lap hasábjain. Először Nagy Andor (PTE, OTDK II. hely): Az e-könyves DRM-technológiák biztonságosságának vizsgálata című dolgozatát olvashatják, a következő számokban pedig Dula Marina (ELTE, OTDK II. hely): Többnyelvű tezauruszok, Girhiny Eszter (DE, OTDK II. hely): Filmelőzetes és kötelező olvasmányok: lehetőség a Z-generáció olvasóvá nevelésére és Kovács Edina (PTE, OTDK III hely): Az adatbányászat alkalmazhatóságának módszerei és lehetőségei a könyvtárakban című írását közöljük. (A szerk.)

Bevezetés

Elektronikus dokumentumok már régóta léteznek, és ahogy fejlődik az informatika, úgy fejlődnek az elektronikus szövegek megjelenítésére alkalmas eszközök is, és nő az ilyen típusú dokumentumok iránti olvasói igény is. Az utóbbi években egyre több elektronikus szöveggel találkozunk. Az elektronikus dokumentumok megjelenése és használata új típusú kihívás elé állítja mind a könyvtárakat, mind a könyvüzemeltetőket. A felvetődő problémák elsősorban szerzői jogi kérdések, mert az elektronikus dokumentumok egyik jellegzetes tulajdonsága, hogy könnyen másolhatók, többszörözhetők. A könnyű másolhatóság az olvasók szempontjából kedvező tulajdonság, ám a jogvédett dokumentumok tulajdonosai aggódva te-

kintenek műveik elektronikus közreadására. Vannak olyan szerzők, akik műveiket nem, vagy csak késleltetve teszik elektronikusan elérhetővé. Más szerzők nem akarnak kimaradni az e-könyvterjesztésből, ezért műveiket elérhetővé teszik elektronikusan, és bíznak az illegális terjesztés megakadályozására létrehozott védelmi megoldásokban.

Kutatásom e védelmi technológiák biztonságosságának vizsgálatára irányult, elsősorban arra, hogy érdemes-e alkalmazni az ún. DRM-technológiákat, és ha igen, melyiket.

A DRM-technológiákat a szellemi tulajdon védelmére fejlesztették ki, használatuk nem új keletű, hiszen már a mágnesszalagos adathordozók is rendelkeztek egyszerűbb adatvédelemmel. Természetesen a mai DRM-technológiák sokkal összetettebb módon mű-

ködni és nem kizárólag a jogvédett tartalom lemásolása akadályozható meg velük.

Azzal a reménnyel kezdtem el a kutatást, hogy választ találok arra a kérdésre, érdemes-e a jövőben DRM-technológiákra támaszkodni az elektronikus könyvek árusítása, illetve könyvtári használata, forgalmazása során, és ha igen, akkor melyik a legbiztonságosabb megoldás.

A DRM fogalma

Az elektronikus adatok másolásvédelmére már az ezredforduló előtt is léteztek törvényi és technológiai szabályozások. Korábban a DRM valóban csak másolásvédelmet jelentett (pl. a műsoros DVD-k tartalmát nem lehet olyan egyszerűen rámásolni a számítógépre, mint mondjuk néhány fényképet egy pendrive-ról). A DRM (Digital Rights Management) digitális jogkezelést jelent. A jelenlegi DRM-technológiák leírásában ma is a Digital Rights Management kifejezést használják, bár szerintem a Digital Restrictions Management¹ kifejezés, ami digitális korlátozásokat jelent, pontosabban fejezi ki, hogy mi a mai DRM-megoldások szerepe. „A DRM a digitális tartalomhoz való hozzáférést lehetővé tevő, illetve szabályozó technikai, műszaki, hardver- és szoftvereszközök összefoglaló neve.”²

Egy e-könyv esetében a DRM nem pusztán az állomány másolását akadályozza meg, hanem az adott technológiától függően több dolgot is korlátozhat: az eszközök maximális számát, amelyen a megvásárolt/kikölcsönzött e-könyv olvasható; az olvashatóság időtartamát (könyvtári e-könyvek esetében ez az olvasóra, megvásárolt e-könyvek esetében arra a személyre vonatkozik, akinek kölcsönadjuk az e-könyvet), szabályozhatja továbbá, hogy hány, illetve mely oldalak legyenek olvashatóak, nyomtathatóak és milyen felbontásban. E korlátozások mellett sok esetben látható és láthatatlan vízjeleket is elhelyeznek az adott dokumentumban, amelyek alapján egyértelműen azonosítható, és visszaélés esetén felelősségre vonható az e-könyv tulajdonosa.

Az eltérő módokon működő DRM-technológiákat több szempont szerint csoportosíthatjuk³. A legelterjedtebb nézet szerint beszélhetünk „hard” vagy más néven „heavyweight DRM”-ről („kemény DRM”), továbbá „soft” vagy más néven „lightweight DRM”-ről („könnyű DRM”), illetve „social DRM”-ről („puha DRM”).

Kemény DRM

Ezt a megoldást kezdték el alkalmazni elsőként az e-könyv-áruházak. A mai napig az Adobe ADEPT névre hallgató megoldása a legelterjedtebb technológia. A hagyományos kemény DRM-megoldások lényege, hogy mire eljut az olvasóhoz a megvásárolt vagy kikölcsönzött e-könyv, többlépcsős hitelesítési folyamaton megy keresztül a központi szerverek közvetítésével. „A hitelesítés célja, hogy a küldő és a fogadó fél egyaránt biztos lehessen a digitális tartalom sértetlenségében (integritásában). A hitelesítéskor egyfajta záradékkal és/vagy digitális aláírással látják el a digitális objektumot.”⁴ A dokumentum minden esetben titkosításra kerül, és csak a megfelelő licenc vagy kulcs birtokában oldható fel. Ebből a felhasználó általában nem lát semmit, viszont az egész folyamat eredménye, hogy korlátozzák az e-könyvvel végezhető műveleteket. A központi hitelesítés hátránya, hogy a felhasználó, ha megvásárolta a tartalmat, függeni fog a könyv-áruháztól. Ha új eszközön szeretné olvasni a dokumentumot (pl. egy új e-könyv-olvasón), akkor ahhoz a webáruház jóváhagyása szükséges, illetve bizonyos DRM-technológiák esetében (pl. Adobe ADEPT) a DRM-technológiát szolgáltató cégnek és a könyv-áruháznak vagy könyvtárnak is hitelesítenie kell a felhasználót, mielőtt megnyithatná az e-könyvet. A DRM-technológia mögött álló cég vagy webáruház/könyvtár megszűnése esetén előfordulhat, hogy a felhasználó egy idő után már nem tudja olvasni az e-könyveit.

Könnyű DRM

A könnyű DRM esetében az e-könyvet a kemény DRM mintájára titkosítják, ám nagyon fontos különbség a két megoldás között, hogy a könnyű DRM esetében mindössze egy jelszó védi a dokumentumot, és ezen kívül semmiféle korlátozást nem alkalmaz. Tehát ugyanúgy másolható, nyomtatható, mint bármely másik fájl, és az olvasására használt eszközök maximális száma sincs meghatározva. Ezt a megoldást rendszerint érzékeny dokumentumok továbbadására használják, az e-könyv-áruházak vagy könyvtárak általában nem alkalmazzák. Ez esetben, amikor a felhasználó megnyitja az állományt, addig nem válik olvashatóvá, amíg be nem írja a dokumentumhoz tartozó jelszót. Rugalmatlanná teszi ezt a megoldást, hogy a jelszóval ellátott dokumentumok nem jeleníthetők meg akármilyen általános célú dokumentum-olvasó szoftverrel, mivel annak támogatnia kell az adott könnyű DRM-technológiát. Ilyen technológiája az Adobe-nak is van.

Puha DRM

Ez a megoldás egyre népszerűbb, mégpedig azért, mert ellentétben az ismertett megoldásokkal, a puha DRM-mel ellátott e-könyvek nem igényelnek speciális szoftvert az olvasáshoz, tehát az egyes e-könyváruházak/könyvtárak konkurens e-könyv-olvasói mindegyikén olvashatóak. Ez úgy lehetséges, hogy az e-könyvek nincsenek titkosítva, tehát az e-könyvolvasó szoftver részéről nem igényelnek speciális tulajdonságokat, melyek értelmezni tudják a titkosítást vagy képesek kommunikálni a hitelesítő szerverekkel. A puha DRM mindössze vízjeleket használ, illetve bizonyos esetekben speciálisan formázza, alakítja a dokumentumot úgy, hogy egyértelműen azonosítható legyen annak tulajdonosa. A puha DRM nem korlátozza az e-könyvvel végezhető műveleteket, viszont megpróbálja elérni, hogy a felhasználó ne adja tovább másnak a megvásárolt vagy kikölcsönzött e-könyvet.

Hipotézis

Abból a megállapításból kiindulva, hogy sok könyvkiadó és szerző nem szívesen publikálja kiadványait elektronikus formában, a következő hipotézist fogalmaztam meg: jelenleg nem létezik olyan DRM-megoldás, amely teljes biztonsággal képes lenne megakadályozni az e-könyvek illegális terjesztését. Ezért e technológiák működésének megismerése és azon elemeknek feltérképezése volt célom, amelyek miatt nem elég hatékonyak a kalózmásolatokkal szemben. Szerintem ugyanis, nem lehetetlen olyan megoldást létrehozni, amely teljes mértékben megakadályozza az e-könyvek kalózmásolatának elkészítését, de ez csakis szigorú szabályrendszerek és korlátozások alkalmazásával érhető el, és az ilyen korlátozások általában negatív hozadéka is van. Jelenleg a legnépszerűbb DRM-megoldások mindegyikének van valamilyen negatív velejárója, amely a legális e-könyvhasználókat hátrányosan érinti (pl. csak meghatározott szoftverekkel olvasható a DRM-mel ellátott e-könyv), miközben az illegális másolatot letöltők teljes szabadságot élveznek. Úgy vélem, hogyha egy DRM-technológia nem éri el a célját, akkor használata felesleges, és a köztes út nemcsak, hogy szükségtelen, de kerülendő is, tehát vagy érje el a célját egy DRM-megoldás, vagy ne használjuk.

Vizsgálati módszerek

Célzottan a kutatási témámhoz illeszkedő magyar nyelvű szakirodalommal kevésbé találkoztam. Sze-

rencsére *Tószegi Zsuzsanna* rendkívül alaposan körüljárja azokat a fogalmakat, amelyek a DRM-technológiák alapját képezik⁵, és segítségemre voltak angol és német nyelvű szakcikkek, valamint blogbejegyzések is. Témám egészét átölelő publikációk híján azonban más utat kellett találnom a DRM-megoldások működésének feltárására és gyenge pontjaiknak a feltérképezésére.

Dokumentációelemzés

Az első módszer, amit alkalmaztam, a DRM-rendszerekhez írt hivatalos dokumentációk értelmezése volt. Ezek a dokumentációk többnyire nem publikusak, mert a szerződött ügyfeleknek szólnak, bár sok esetben fellelhetőek az interneten is. A BooXtream DRM vizsgálatakor például sikerült elérnem a projekt vezetőjét is, aki készséggel válaszolt a technikai jellegű kérdéseimre, és néhány szabadon nem hozzáférhető, főként technikai leírásokat tartalmazó dokumentumot is a rendelkezésemre bocsátott. A dokumentációk lényegében azoknak az informatikusoknak szólnak, akik majd telepíteni, konfigurálni fogják az adott DRM-technológia használatához szükséges szoftvereket, viszont ezen információk birtokában következtetni lehet arra, hogy az egyes megoldások miképp valósítják meg az e-könyvek DRM-védelmét.

A DRM-védelmet megvalósító szoftverek vizsgálata

Sok esetben a dokumentációs anyagok csak a felszínbe engednek bepillantást, épp csak annyit írnak le, amennyi feltétlen szükséges ahhoz, hogy a rendszert konfiguráló informatikus boldoguljon a beállításokkal. Ám ez épp elég ahhoz, hogy kiindulási alapként szolgáljon a technológia mélyebb megismeréséhez. Ezért második kutatási módszerem a DRM-védelmet megvalósító szoftverek vizsgálata lett.

Amikor elindítunk egy programot vagy csak megnyitunk egy mappát az operációs rendszerben, az fájlműveletekkel jár, még ha ezek a felhasználó számára láthatatlanok is. Ezek a fájlműveletek nyomon követhetőek, és megfigyelésükkel, illetve a létrehozott fájlok elemzésével fény derülhet az adott DRM-technológia működésének részleteire. Példának okáért, amikor megnyitunk egy Marlin DRM-mel ellátott e-könyvet, akkor egy rejtett rendszermappában apró szöveges fájlok jönnek létre, melyeket átolvasva megállapítható, hogy a Marlin az e-könyvek titkosí-

tását milyen eljárással oldja meg. Továbbá a hálózati kártya forgalmát megfigyelve bepillantást nyerhetünk a számítógépünk és a hitelesítő szerverek között közlekedő adatsomagokba, melyekből további hasznos információk nyerhetők ki a technológia alaposabb megértéséhez.

A sebezhetőségeket kihasználó szoftverek vizsgálata

Hogyha valaminek a biztonságosságát vizsgáljuk, célszerű megnézni azokat a megoldásokat, amelyek sikerrel cáfoltak rá valaminek a biztonságára, és az alkalmazást a gyakorlatba is átültették. Esetünkben olyan scriptekről, programokról van szó, amelyeket a készítőik azért publikáltak, hogy eltávolítsák egy-egy e-könyv DRM-védelmét. Ha egy megoldás nyílt forráskódú, tehát szabad bepillantást enged a forráskódba, akkor a legegyszerűbb magát a programkódot átböngészni, illetve nyomon követni a programsorok végrehajtásának körülményeit. Kutatásom harmadik módszere ezért a világhálón szabadon fellelhető, kész DRM-védelmek eltávolítására létrehozott scriptek, programok vizsgálatára irányult, mert ezekből következtetni tudtam nemcsak az adott technológia működésének elemeire, hanem a sebezhető pontokra is fény derült.

Kiválasztottam nyolc olyan DRM-technológiát, amelyek alkalmazhatók e-könyvekre és a mai napig folyamatos a fejlesztésük és karbantartásuk, majd az említett módszerekkel elvégeztem az elemzésüket. Az átvizsgált DRM-technológiák a következők voltak: Adobe ADEPT DRM, Apple FairPlay DRM, Barnes and Noble DRM, Marlin DRM, BooXtream DRM, SiDiM DRM, Amazon DRM-ek (mobi-DRM, topaz-DRM).

A továbbiakban egy nyílt forráskódú modellen, a BooXtream DRM-en mutatom be az elemzés menetét: először ismertetem a modellek működését, majd rámutatok a technológia gyenge pontjaira. (A cikk elektronikus változatában mind a nyolc DRM-technológia bemutatása, elemzése elolvasható.)

BooXtream DRM – „social DRM”

A BooXtream DRM az egyik legfrissebb jövevény e technológiák piacán. A hagyományos DRM-technológiák megpróbálnak minél szigorúbb szabályrendszereket, minél nehezebben feltörhető titkosításokat és bonyolult algoritmusokat alkalmazni annak érdekében, hogy megnehezítsék a kalózmásolatok

terjedését. Az elképzelés nem rossz, ám függetlenül attól, hogy egy DRM-technológia mennyire fejlett és összetett, mindig lesz bennük olyan biztonsági rés, amelyet a crackerek kihasználhatnak, és ki is használnak. Annak fényében, hogy egy-egy DRM-technológia használata forintban kifejezve több millióba kerül évente, érthető, hogy egyre több kiadó teszi fel a kérdést: van-e értelme olyan DRM-védelemért fizetni, amely ilyen könnyedén kijátszható?

A kérdés feltevése után három dolgot tehetnek. Az egyik, hogy késleltetve, esetleg egyáltalán nem adják ki a legnépszerűbb kiadványaikat elektronikus formában, mint ahogy teszi ezt Stephen King bizonyos regényeivel. Ezt a megoldást a legnagyobb hollywoodi filmstúdiók már régóta alkalmazzák. Figyelik minden ország kalózfilm-piacát, és ahol rendszeresen felkerülnek a filmjeik a vetítés alatt vagy már azt megelőzően, ott szankciókat alkalmaznak, ilyen a késleltetett premier. Magyarországon jelenleg is később kerülnek bemutatásra a Disney filmjei, ami nem meglepő, hiszen – ha lehet így fogalmazni – az egyik legnagyobb kalózbirodalom vagyunk.

A másik lehetőség, hogy DRM nélkül terjesztik az e-kiadványaikat, mondván, hogy csak kidobott pénz a védelemre áldozni. Sokan élnek ezzel a lehetőséggel, és a felhasználók körében valóságos mozgalommá nőtte ki magát a DRM-védelmet ellenző nézet, melynek legfőbb gondolata, hogy a DRM-ből úgysem profitálnak a kiadók, viszont a korlátozások megnehezítik azok dolgát, akik legalisan vásárolnak ilyen kiadványokat.

A harmadik út a „social DRM”-re váltás. Ezt lépte meg a Harry Potter-könyvek kiadója is⁶. Ahelyett, hogy kiadványait a legnagyobb e-könyvúrházakban terjesztené egy hagyományos DRM-védelemmel ellátva, saját weboldalt indított Pottermore néven, ahol egy holland programozó/üzletember, *Huub van de Pol* BooXtream nevű technológiáját használja. A technológia nem új fejlesztés, a holland Icontact vállalat DRM-megoldását alakították át e-könyvekhez. A megoldás a legváltozatosabb módon tűzdeli meg vízjelekkel a dokumentumot, és mindegyik vízjel alapján beazonosítható a vásárló. Ezzel a megoldással a Barnes and Noble is él, ám nem kifejezetten erre a célra fejlesztett DRM-technológiát használ, így jóval kevésbé hatékony, és könnyebben fellelhetőek a vízjelek. A BooXtream nagy előnye a konkurens DRM-megoldásokkal szemben, hogy jóval alacsonyabb áron kínálja megoldását, ráadásul az e-könyvúrház, esetleg könyvtár részéről minimális szoftveres módosítás szükséges a meglévő rendszerükön. A szol-

gáltatásnak nincs rendszeresen kifizetendő díja, mint pl. az Adobe ADEPT megoldásánál, hanem az eladott e-könyvek után kell fizetni. Ez az összeg az eladott e-könyvek számától függően 0,125–0,50 euróig terjed, és a technikai segítségnyújtás is díjmentes.

A BooXtream kétféle e-könyv formátummal kompatibilis, ezek az *epub* és *mobi*. Amikor valaki megvásárol egy ilyen DRM-technológiával ellátott e-könyvet, majd elindítja annak letöltését, akkor a BooXtream szoftvere vízjelekkel látja el a dokumentumot, és csak miután végzett, azután adja át a felhasználónak. Ez mindössze néhány másodpercet vesz igénybe. Mind az *epub*, mind pedig a *mobi* ún. konténer-formátumok, tehát nem egyetlen, hanem több tucatnyi fájlból tevődnek össze, melyeket a felhasználó csak egy egységes *epub*- vagy *mobi*-kiterjesztésű fájlnek lát. Nem véletlen, hogy a BooXtream választása e-fájlformátumokra esett, hiszen amellett, hogy a legelterjedtebbek, a belső fájlszerkezetük lehetőséget ad a vízjelek elrejtésére.

Sokan nemcsak azért fogadták örömmel az új technológia érkezését, mert egy merőben más megközelítést alkalmaz a hagyományos DRM-technológiákhoz képest, hanem azért is, mert a Kindle-re, a legnépszerűbb e-könyvolvasóra eddig egyedül az Amazon webáruháza kínált DRM-mel ellátott e-könyveket. A kiadók – amennyiben el akartak érni a Kindle tulajdonosokhoz – kénytelenek voltak az Amazonon keresztül eladni DRM-mel védett kiadványaikat. A BooXtream ezen szeretett volna változtatni, így az *epub*-szabvány mellett a *mobira* is implementálta a technológiát. Azért pont erre, mert a formátumot úgy képesek kezelni a Kindle eszközök, hogy a BooXtream DRM-e sem okoz fennakadásokat. Tehát ha egy kiadónak megfelel ez a DRM-védelem, akkor úgy tudja magát függetleníteni az Amazontól, hogy a Kindle tulajdonosok vásárlóközönségét is megtarthatja.

Ellentétben a Barnes and Noble „social-DRM” megoldásával, a BooXtream nem helyez el személyes adatokat a fájlokban, viszont így is egyértelműen azonosítható, hogy mely e-könyv, mely felhasználóhoz tartozik. Ennek az az oka, hogy amikor a Barnes and Noble bejelentette, hogy a vásárlók bankkártyaszámát is vízjelként fogja felhasználni, akkora tiltakozási hullámot váltott ki, melynek eredménye az lett, hogy néhány nap után már több olyan eszköz is megjelent, amely a vízjeleket hivatott eltávolítani. Tehát a BooXtream, ahogy a hirdetéseiben is írja: egy sokkal kevésbé toladó, személyiségi jogokat nem sértő DRM-technológiát fejlesztett ki, amely nem nehe-

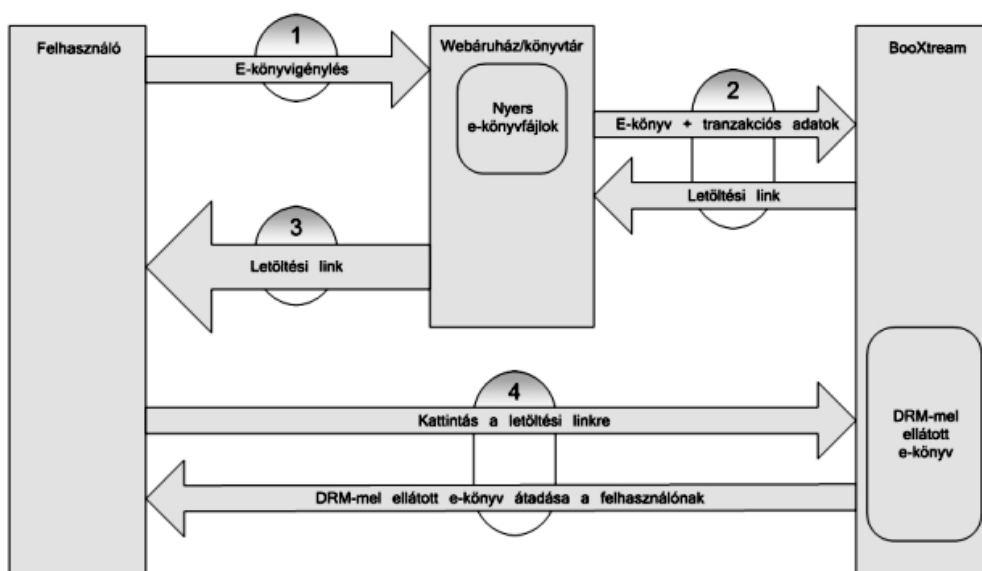
zíti meg azok dolgát, akik legálisan vásárolták meg az e-könyvet és több eszközön is szeretnék olvasni, esetleg ismerőseiknek odaadni. Kérdés, mi van akkor, ha valaki egy nyilvános számítógépen felejt a fájlt, vagy valamilyen más módon kikerül a keze közül? A felhasználási feltételekben benne van, hogy a vásárló maga felel azért, hogy az e-könyv ne kerüljön a nyilvánosság elé, és pontosan ez a „social-DRM” lényege: megpróbálja elvenni a felhasználó bátorságát az e-könyv közkézre adásától.

A BooXtream modell működése

A vállalat kétféle megoldást kínál az e-könyvek DRM-védelemmel való felvértezésére, és a kétféle megoldás is tovább bontható két-két némiképp különböző megvalósítási formára. Mindegyik megoldás során ún. API-n keresztül zajlik a teljes DRM-ezési folyamat. Ez azt jelenti, hogy a BooXtream szerveréhez *http*-protokollon keresztül kerülnek a szükséges információk (pl. felhasználói- és vásárlási azonosítók és maguk az e-könyvfájlok is), amelyre egy XML-dokumentumban válaszol, és ez a XML-dokumentum tartalmaz minden szükséges információt, illetve a felhasználó számára szükséges letöltési linket is. A megoldás előnye pl. az Adobe ADEPT-tel szemben, hogy a terjesztőnek nem szükséges speciális szoftvereket telepítenie vagy külön szervereket beüzemeltetnie erre a célra. Mind a folyamathoz szükséges hitelesítési lépések, mind pedig az e-könyvfájl vízjelekkel való ellátása a BooXtream szerverén zajlik.

☛ *1/a) megvalósítás: csak a nyers e-könyvállomány van a terjesztő szerverén (Lásd 1. ábra.)*

Ebben az esetben a DRM-mel ellátott e-könyvek minden esetben a BooXtream szerverén helyezkednek el, és az e-könyvárúháznak vagy könyvtárnak mindössze letöltési linkeket és a nyers e-könyvállományokat kell kezelnie, amelyeken keresztül a felhasználó eléri az adott dokumentumot. Ennek a megoldásnak „delivery platform mode” a neve, a delivery vagyis kézbesítő szóval utalva arra, hogy a webáruház/könyvtár csupán kézbesítő szerepet játszik, a felhasználó nem közvetlenül a BooXtream szerverével létesít kapcsolatot a letöltés során. Először leadja a megrendelését a webáruháznak/könyvtárnak, amely a jóváhagyást követően összecsomagol minden olyan információt, amely a vízjelek előállításához szükséges, valamint magát az e-könyvfájlt is, és az API-n keresztül eljuttatja a BooXtream szerverének. A szerveren futó szoftver ekkorra még csak egy letöltési linket hoz létre, melyet a felhasználó a terjesztő továbbításával



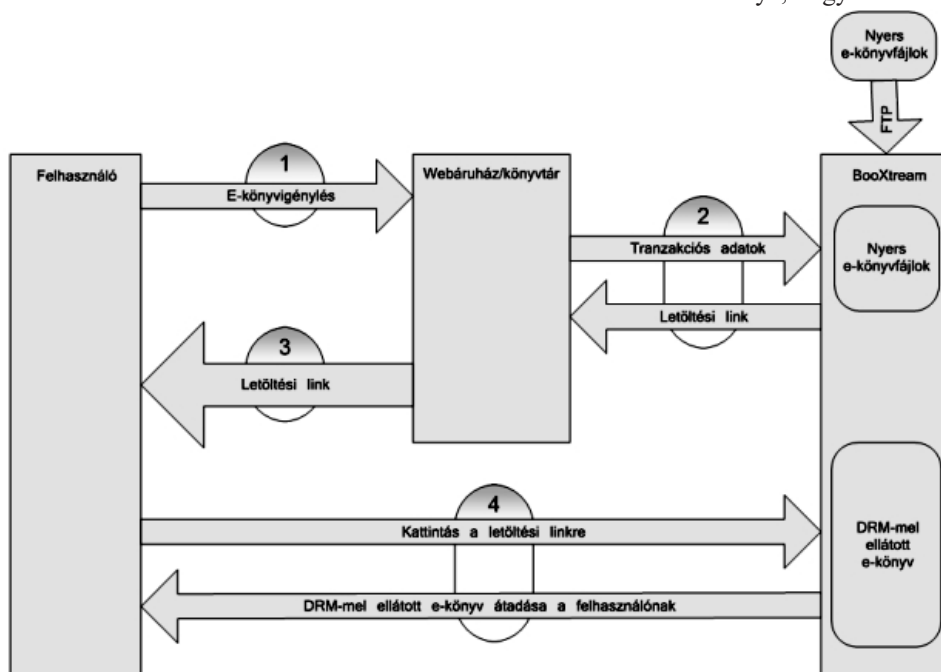
1. ábra

A BooXtream 1/a. rendszeréhez kapcsolódó folyamatábra, amely a BooXtream API használatának folyamatát mutatja be. Kezdő- és végpontja a felhasználó (olvasó).

kap meg. Miután rákattint, kommunikációs csatorna jön létre a felhasználó számítógépe és a BooXtream szervere között, majd az e-könyv DRM-ezése után a felhasználónak lehetősége lesz letöltenie a vízjelekkel ellátott dokumentumot.

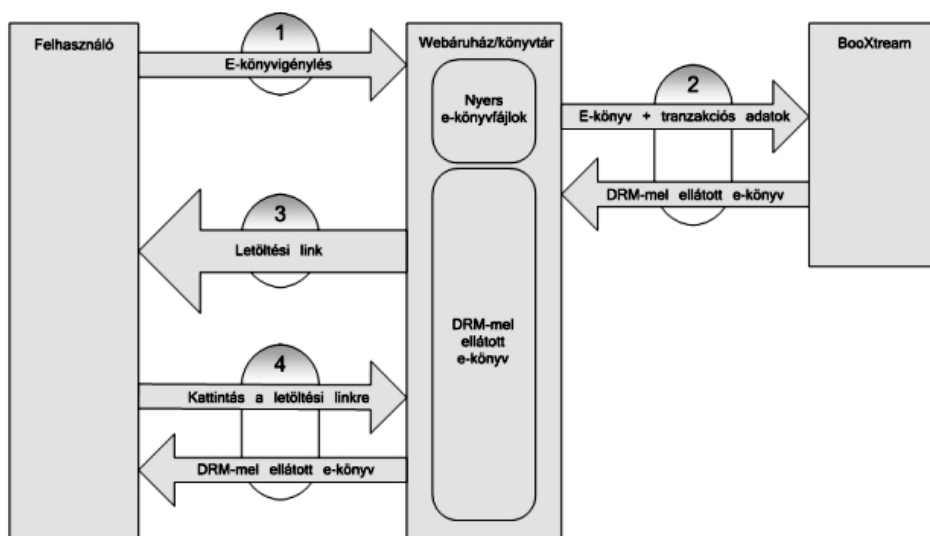
© 1/b) megvalósítás: a terjesztő szerverén kizárólag letöltési linkek tárolódnak (Lásd 2. ábra.)

Ez a modell annyiban tér el az előbbtől, hogy a terjesztő előre feltölti az összes e-könyvét a BooXtream szerverére. Ennek előnye, hogy a felhasználó vala-



2. ábra

A BooXtream 1/b. rendszeréhez kapcsolódó folyamatábra, amely a BooXtream API használatának folyamatát mutatja be. Kezdő- és végpontja a felhasználó (olvasó).



3. ábra

A BooXtream 2/a. rendszeréhez kapcsolódó folyamatára, amely a BooXtream API használatának folyamatát mutatja be. Kezdő- és végpontja a felhasználó (olvasó).

mivel gyorsabban kézhez kapja a vásárolt vagy kölcsönzött dokumentumot, illetve a terjesztőnek nem a saját infrastruktúráján kell megoldania az e-könyvek tárolását. Igaz, ezért valamivel többet kell fizetnie a BooXtreamnek.

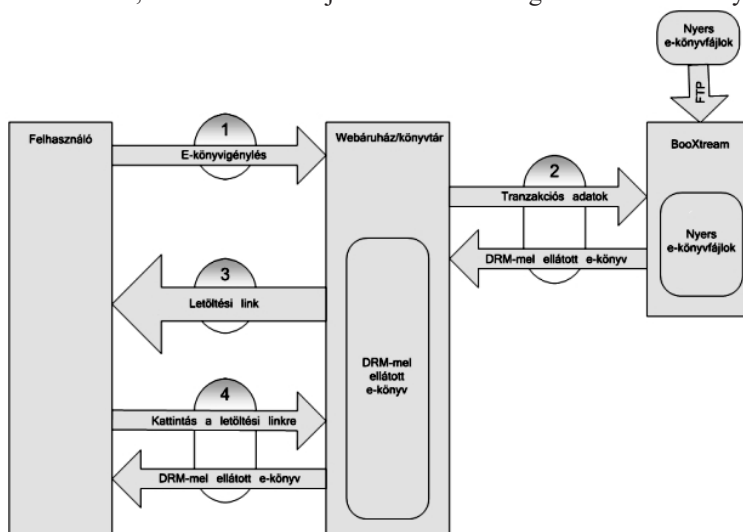
© 2/a) megvalósítás: a terjesztő szerverén a nyers és DRM-mel ellátott e-könyvfájlok megtalálhatóak (Lásd 3. ábra.)

A következő sémának „direct mode” a neve, vagyis a felhasználó egyetlenegyszer sem létesít kapcsolatot a BooXtream szerverével, ezt a munkát teljes

egészeben a terjesztő szervere végzi, természetesen a BooXtream API-n keresztül. A felhasználó szempontjából annyi a különbség az 1/a. megoldáshoz képest, hogy az e-könyvet a terjesztő szerveréről fogja letölteni, mivel annak átadását a terjesztő nem bízta rá a BooXtreamre, csupán a DRM-ezési folyamatot végezteti el vele az API-n keresztül.

© 2/b) megvalósítás: a terjesztő szerverén csak a DRM-mel ellátott e-könyvfájlok tárolódnak (Lásd 4. ábra.)

A különbség itt mindössze annyi a 2/a. megoldáshoz



4. ábra

A BooXtream 2/b. rendszeréhez kapcsolódó folyamatára, amely a BooXtream API használatának folyamatát mutatja be. Kezdő- és végpontja a felhasználó (olvasó).

képest, hogy az 1/b. séma mintájára a nyers e-könyv-fájlokat előre feltöltik a BooXtream szerverére.

A BooXtream vízjelezési eljárásnak gyakorlati megvalósulása

A BooXtream szoftvere elhelyez az e-könyvekben egyaránt látható és láthatatlan vízjeleket. A látható vízjelek (pl. az ex libris), amelyek tartalmazzák a felhasználó egyedi azonosítóját és egy szerzői jogi oldalt, amely felhívja az olvasó figyelmét arra, hogy dokumentumot ne adja tovább. A láthatatlan vízjelekből több is van, csak néhány példát emelnék ki: a vásárló neve, e-mail címe és rendelési azonosítója egyaránt felhasználásra kerül. Ezekből egy egyszerű algoritmus egy-egy kódsort generál, és több helyen is elhelyezi őket az e-könyvben. Ilyen hely

az *epub/mobi-konténerekben* lévő fájlok neve, a CSS-stílusfájlok és az e-könyv oldalain fellelhető képek. Ez nem úgy néz ki, mint amikor egy fotóműhely a kép sarkába illeszti a logóját, hanem a szteganográfia módszerével élve, a kép hexadecimális kódjába kerül be egy kódsor, amely a kép megjelenítésekor láthatatlan. „A szteganográfia (szó szerint: „fedett írás”) lényege, hogy a titkos információt valamilyen digitális adathalmazban (pl. képen) rejtik el.”⁷ Példa erre az 5. ábra keretben kiemelt részében elhelyezkedő hexadecimális kódrészlet, amely sztringgé átalakítva „303138343830333100000000”- Ez lehet például a felhasználó egyedi azonosítója vagy akár a bankkártya száma is. Tehát ez esetben a vízjel az 5. ábra keretben kiemelt részében található képfájlba van beágyazva, és anélkül távolítható el annak hexadecimális kódjából, hogy sérülne a kép.

c4	3c	f5	01	c1	3c	29	c9	03	f1	a2	8a	1b	b3	b2	04
ae	c2	df	ed	bf	68	79	ae	63	46	46	39	8d	7a	12	69
e6	d5	b7	1b	a9	57	0b	9c	85	c8	fd	28	a2	84	b4	0d
98	d9	5a	33	ba	57	b6	0a	b8	e3	2b	de	87	53	e6	2b
6d	c2	8c	67	9f	e9	45	15	2c	6f	46	32	ee	48	98	12
63	06	3c	f3	90	7a	fd	3f	ad	56	11	f9	ab	f6	7b	6b
60	2d	d2	3c	ab	6e	e3	af	4a	28	a8	7a	c8	6b	61	6e
66	96	75	32	08	9f	c9	84	ff	00	cb	32	79	c7	6c	77
a2	4b	d8	c3	2b	3f	cb	1b	20	00	30	c1	dd	e9	45	15
9d	59	ca	2a	e8	a8	a4	c1	84	b3	49	e5	aa	7c	9b	4f
41	85	19	ed	ef	52	ef	8e	2f	2e	d9	60	e0	8f	9c	21
e3	38	fd	68	a2	b4	4e	c4	b5	a9	cd	7c	4a	b2	f3	74
82	a6	15	75	57	56	7f	35	4b	2a	0e	cc	71	cf	1e	9d
eb	c4	3f	68	ef	1e	68	7f	0f	3e	14	78	cf	c5	3e	39
d2	27	6d	1f	47	f0	94	d7	9a	dc	a6	2d	cb	35	b9	8c
af	94	8a	0e	46	7a	d1	45	79	d9	86	97	6b	b7	e8	cf
ab	e1	4a	10	c6	66	d8	6c	3d	4f	86	75	21	17	6d	1d
a5	38	27	6f	3b	3d	3c	cf	e7	26	47	82	59	9e	5b	68
3c	a8	9e	46	68	a2	ce	76	21	24	85	fc	06	05	14	51
5f	22	7f	aa	56	b6	87	ff	d9	33	30	33	31	33	38	33
34	33	38	33	30	33	33	33	31	30	30	30	30	30	30	30

5. ábra

A BooXtream rejtett vízjelezési eljárását bemutató példa. Az ábrán egy JPEG-képfájl részletének hexadecimális kódja látható.

A modell gyenge pontjai

Mivel a BooXtream lehetőséget ad a technológiáját használó könyvterjesztőknek arra, hogy a vízjeleket testre szabják, ezért nem lehet egyetlen séma alapján valamennyi BooXtreamet használó könyvtárház DRM-védelmét eltávolítani, de néhány óra munkával és megfelelő háttérismerettel felismerhető valamennyi látható és láthatatlan vízjel. A legnépszerűbb vízjelező algoritmusok megkerülésére számos szabadon hozzáférhető szoftver létezik, de a BooXtream vízjeleinek eltávolításához (még) nincs ennyire „felhasználóbarát” megoldás.

A megfelelő DRM kiválasztása

Nem minden e-könyves DRM-technológia alkalmazható valamennyi területen. Jelenleg összesen nyolcféle aktívan fejlesztett megoldás használható az e-könyvek DRM-védelmére, ezek közül egy (a SiDiM) csak német nyelvű dokumentumokkal kompatibilis.

Saját publikáció e-könyves terjesztése

Aki saját e-könyvét szeretné eladni, annak első lépésként el kell döntenie, hogy szükségét érzi-e valamilyen DRM-megoldás használatának. Ha nem, akkor

regisztrálhat olyan webáruházhoz, ahol nem kötelező aktiválni a DRM-védelmet, és egy csekély jutalék fejében az e-könyve megtalálható lesz a webáruház kínálatában (pl. Amazon), esetleg alternatív utakat választ e-könyvének terjesztésére (pl. saját weboldal). Amennyiben valaki DRM-védelemmel szeretné árusítani e-könyvét, akkor ugyancsak választhatja valamelyik meglévő e-könyvárúházt, vagy saját weboldalon saját maga valósíthatja meg a védelmet. Ehhez igénybe veheti a Marlin, Adobe ADEPT, SiDiM és BooXstream megoldásait. Ezek közül az ADEPT rendkívül költséges saját használatra, a SiDiM csak német nyelven működik, a Marlin pedig ugyancsak túl költséges, ha nem saját infrastruktúrára működ-tetjük (ami egyébként ugyancsak extra költséggel járna). Ebből kiindulva saját használatra marad a BooXstream, hiszen használatához nem szükséges saját infrastruktúra, és az igénybevételének díja a legkedvezőbb a konkurensékhöz képest.

Saját e-könyvárúház

Saját e-könyvárúház indítása esetén a kiadóktól függ, hogy milyen DRM-megoldást kénytelen használni a tulajdonos, ez a legtöbb magyar és külföldi webáruház esetében az Adobe ADEPT megoldása, amely egyben a legdrágább is. Ennek oka valószínűleg az, hogy az Adobe a legismertebb név a DRM-technológiák piacán, és igazi, hagyományos kemény DRM-et kínál. A kutatásomból kiderült, hogy e megoldásnak számos biztonsági hiányossága van, és kérdéses, hogy képes-e megakadályozni az illegális másolatok létrehozását. Külföldön már van néhány kiadó, amely hajlik az alternatív megoldások felé (pl. O'Reilly, Tor, Carina Press), Magyarországon erre egyelőre kevésbé látok hajlandóságot a kiadók részéről, pedig véleményem szerint a BooXstream vagy – a kemény DRM-vonalon maradva – a Marlin jobb választás lenne, mint az Adobe ADEPT. Nemcsak azért, mert olcsóbb, hanem mert emellett legalább annyira biztonságos, mint az ADEPT, és ha saját infrastruktúrára üzemeltetjük, akkor nyílt forráskódú megoldás révén egyedi módosításokat is alkalmazhatunk benne.

Könyvtári felhasználás

Mint azt már a kutatásom elején említettem, az e-könyvek könyvtári terjedésének legfőbb oka a kiadók bizalomhiánya. Könyvtári alkalmazásra az ismertett technológiák közül csak az Adobe ADEPT, a Marlin és a BooXstream jöhet szóba, viszont az

utóbbi kettőben nem lehet olvashatósági időlimitet megadni, márpedig ezt a kiadók szükségesnek tartják. Így marad az Adobe ADEPT, illetve sokkal inkább a technológiát felhasználva teljes körű könyvtári rendszert nyújtó vállalatok, mint az OverDrive vagy a 3M. A probléma megint csak a hatékonyság kérdése és a magas ár, amely növeli a kiadásokat, így nem csoda, hogy a könyvtárak nem igyekeznek e-könyvekkel bővíteni az állományukat.

Két lehetséges utat látok, elsősorban a magyar könyvtárakra vonatkoztatva. Az egyik egy saját kemény DRM-megoldás kifejlesztése vagy a Marlin DRM módosítása könyvtári használatra. Egy egyszerűbb kemény DRM-megoldás megalkotása nem járna túl sok programozói munkaórával. Az előnye lenne, hogy nem kellene használati díjat fizetni egy külső vállalatnak, és mivel a széles körben használt Adobe ADEPT DRM-védelmének eltávolításához számos eszköz áll az olvasók rendelkezésére, így egy saját megoldás semmivel sem lenne kevésbé hatékony. Sőt, a kisebb számú felhasználói közösség talán kevésbé lenne vonzó célpontja a crackereknek. A másik megoldás a puha DRM-ek használata lehetne, de ezeknél nincs megoldva a kölcsönözhetőségi időtartam beállíthatósága, így könyvtári alkalmazása esetén mindenképp további fejlesztéseket igényelne.

A DRM-et övező problémák és javasolt megoldások

Problémák

Kutatásom elején megfogalmaztam azt a hipotézist, hogy jelenleg nem létezik olyan DRM-technológia, amely teljes biztonsággal képes lenne megakadályozni egy e-könyv illegális terjesztését. Mindegyiknek vannak olyan sebezhető pontjai, amelyeket a crackerek képesek kihasználni. A kemény és könnyű DRM-megoldásoknál két fő sebezhető pont jelenik meg: a titkosítást feloldó kulcs viszonylag egyszerű előállíthatósága, illetve a túl kevés karaktert tartalmazó kulcsok brute force-módszerrel való megfejthetősége. A puha DRM sebezhetősége abban rejlik, hogy a vízjeleket akkor is meg lehet különböztetni az eredeti szövegtől, ha azok olvasásához szükséges valamilyen speciális program, tehát a legtöbb olvasó számára láthatatlan vízjeleket használnak a készítők. A jelenlegi DRM-megoldások közül egyedül a SiDiM által alkalmazott egyénesített e-könyvek jelenthetnek fejtörést a crackerek számára, ám a lehetőség itt is nyitott. Ráadásul a SiDiM-ről szóló kritikákat olvasva az a véleményem, hogy a megoldás nem fog

széles körben elterjedni, ezt az is alátámasztja, hogy – valószínűleg az elutasító fogadtatás hatására – a fejlesztők régóta nem hallattak magukról.

A fő problémát abban látom, hogy kevés e-könyvekre alkalmazható DRM-technológia létezik, és eltekintve az Amazon e-könyvruházról, a legtöbb jelentős e-könyvruház és könyvtár az Adobe ADEPT megoldását vagy annak egy módosított változatát használja. Úgy vélem, hogy az Adobe komoly vetélytársak híján lomhává vált, és nincs motiválva a DRM-megoldásának biztonságosabbá tételében. Pedig hogyha rendszeresen, évente többször változtatna a kulcsfájllelőállító-algoritmusán, illetve még összetettebbé tenné azt, akkor jelentősen megnehezítené a crackerek dolgát. Az Amazon *topaz* DRM-ének esetében is majdnem két év kellett⁸, mire nyilvánossá vált a kulcsfájllelőállító algoritmus.

Bár kutatásomnak nem célja a sebezhetőségek mögött álló okok feltárása, de felmerül a kérdés, kinek áll érdekében egy teljesen biztonságos DRM-megoldás létrehozása. Az e-könyvek jogtulajdonosainak valószínűleg igen. És az e-könyvruházaknak és a velük szerződött DRM-technológiák előállítóinak? A kemény DRM-megoldásoknak – mint már említettem – számos negatív hozadéka van az e-könyveket legálisan megvásároló olvasókra nézve. Egy kemény DRM-mel ellátott e-könyv nem olvasható akármilyen e-könyvolvasó eszközön vagy szoftveren, illetve más formátumba se konvertálható át, ráadásul az olvasó a DRM miatt mindig függeni fog az e-könyvruházról, hiszen ha új eszközön szeretne olvasni egy korábban megvásárolt e-könyvet, akkor azt hitelesítenie kell az e-könyvruház szerverén keresztül. Így lényegében soha nem lesz teljesen a sajátja a megvásárolt e-könyv, nem tudja úgy elajándékozni vagy eladni valakinek, mint egy papír formátumú könyvet, ráadásul kérdéses, hogy mi történik az e-könyvruház megszűnésekor.

Arra a kérdésre, hogy van-e olyan DRM-technológia, amelyben teljesen megbízhatunk, a válasz az, hogy nincs, még a legnépszerűbb Adobe ADEPT is sebezhető; sőt – valószínűleg az elterjedtsége miatt – az ADEPT DRM-e távolítható el legegyszerűbben, mivel erre számos ingyenesen elérhető, felhasználóbarát felülettel rendelkező eszköz áll rendelkezésre. Tehát hiába költ valaki DRM-re, az nem képes betölteni a funkcióját.

Javasolt megoldások

Felmerül a kérdés, hogy az elmondottak tudatában

van-e értelme DRM-technológiát alkalmazni, hiszen a kalózkodást nem fogja vissza, és aki képes valamelyik fájlcsereelő oldalra e-könyvet feltölteni, annak valószínűleg a DRM-védelmek eltávolítása sem okoz különösebb nehézséget, így az illegálisan elérhető tartalmakat fogyasztók dolgát nem, viszont a legális forrásokat igénybevevők dolgát megnehezíti a DRM.

Bodó Balázs, akinek egyik legismertebb publikációja a *Szerzői jog kalózzai* c. könyv, 2010-ben tartott egy előadást „*A DRM mítosz – mire jó és mire nem a másolásvédelem?*” címmel⁹. Véleményem egybeeseng az előadóéval: a DRM nemcsak pénzkidobás, de a céljával ellenkező hatást válthat ki. A DRM eredeti célja az illegális terjesztések megakadályozása és ezzel együtt a legális források vonzóbbá tétele. Vonzóbbá tétele egyrészt a fogyasztók számára, hiszen hogyha az e-könyv nem szerezhető be illegális forrásból, akkor marad a legális alternatíva; másrészt a kalózkodástól tartó kiadók számára. A gond az, hogy – a jelen kutatás szerint – nem létezik megbízható DRM-megoldás.

Egy lehetséges megoldásnak az egyes e-könyvruházak és könyvtárak által saját célra kifejlesztett kemény és puha DRM-et ötvöző megoldásaiban látom, amelyek kulcsfájllelőállító és egyéb biztonsági célú elemei folyamatosan változtatva lennének, így jelentősen megnehezítve a crackerek dolgát. A másik megoldás a mindennemű DRM-technológia használatának mellőzése. Akik emellett az út mellett érvelnek, úgy gondolják, hogy a DRM nem szab gátat az illegális másolatoknak, viszont sokakat eltántorít a legális e-könyvvásárlástól, mivel az illegális másolatokban nem érvényesülnek a korlátozások. Állításuk szerint a DRM-megoldások teljes mellőzése nemcsak, hogy nem hatna negatívan az e-könyvpiacra, de növelné annak forgalmát is. Mindemellett nagyon fontosnak tartom, hogy a kalózoldalaknak legyen olyan legális alternatívájuk, amelyek könnyen vagy könnyebben kezelhetők. A zeneiparban már bebizonyosodott, hogy a legális forrás hiába lesz mindig drágább a teljesen ingyenes illegális forrásnál, igény akkor is van rá. Amióta megjelentek az igazán jól használható zenevásárló weboldalak (pl. Spotify, Deezer, Google Play Music), a zenekiadók bevétele folyamatosan nő, de így van ez a filmiparban is, az online nézhető filmeket szolgáltató Netflix már magasabb bevétellel rendelkezik, mint pl. az HBO¹⁰.

Úgy gondolom, hogy az illegális másolatok csak akkor vannak negatív hatással a jogtulajdonosok bevételeire, hogyha az illegális forrásoknak nincs

versenyképes legális alternatívájuk. Látszik, hogy hiába van rengeteg kalózkodó, ahol teljesen ingyen beszerezhető a legtöbb film és zene, mégis egyre nő azok száma, akik inkább a legális forrásokat részesítik előnyben. Példának okáért a legnagyobb, legális filmvásárlásra lehetőséget adó Netflix¹¹ és az egyik legnagyobb online zeneáruház, a Spotify¹² is folyamatosan növelni tudja forgalmát. Tehát a kiadókra esetlegesen káros hatással bíró illegális e-könyvtöltések visszaszorítása véleményem szerint nem a DRM-technológiák alkalmazásával, hanem a versenyképes legális források előállításával érhető el.

Felhasznált irodalom

1. ABIE, Habtamu: Frontiers of DRM knowledge and technology = IJCSNS International Journal of Computer Science and Network Security, 2007. 7. évf. 1. sz. 216–231. p.
2. Adobe Inc.: Adobe and Barnes & Noble Join Forces to Standardize eBook Technology. 2009. https://www.adobe.com/aboutadobe/pressroom/pressreleases/pdfs/200910/102009AdobeBarnesNoblebooks_000.pdf (2015. június 15.)
3. Adobe Systems Incorporated: Adobe Content Server 4 User Manual. 2009. [ügyfeleknek szánt nem publikus dokumentum]
4. AUSDERAU, Patrick: Protection mechanisms for electronic books. Helsinki Metropolia University of Applied Sciences, Helsinki, 2014. [doktori disszertáció] https://www.theseus.fi/xmlui/bitstream/handle/10024/74667/Ausderau_Patrick.pdf (2015. június 15.)
5. BAILEY, Jonathan: Changing Words and Changing Direction on eBook DRM. PlagiarismToday.com, 2013. 06. 18. <https://www.plagiarismtoday.com/2013/06/18/changing-words-and-changing-direction-on-ebook-drm> (2015. június 15.)
6. Bangor University's Languages Technologies Unit: E-publishing: Technical guidelines for Publishers in Wales. 2012. http://techiaith.bangor.ac.uk/e-gyhoeddwr/wp-content/docs/E-publishing-Technical_Guidelines.pdf (2015. június 15.)
7. BIRYUKOV, Alex – LEURENT, Gaëtan – ROY, Arnab: Cryptanalysis of the „Kindle” Cipher. Luxembourg, 2012. http://www.di.ens.fr/~leurent/files/Kindle_SAC12_slides.pdf (2014. július 25.)
8. BODÓ Balázs: A DRM-mitosz – mire jó és mire nem a másolásvédelem. In: Könyvmarketing konferencia, Budapest, 2010. <https://prezi.com/ecqe-mxidnuz/konyvmarketing-2010> (2014. december 7.)
9. DEMARCO, Amanda: BooXtream on „Social DRM” as a Better Option for E-books. 2012. <http://publishingperspectives.com/2012/09/booxtream-on-social-drm-as-a-better-option-for-e-books/> (2014. október 25.)
10. DE-MULDER, Yoni: White-Box Cryptography. Belgium, 2014. <https://www.cosic.esat.kuleuven.be/publications/thesis-235.pdf> (2014. július 25.)
11. Digital Watermarking Alliance: Digital Watermarking as a Proposed Solution to Orphan Works. 2007. http://www.digitalwatermarkingalliance.org/docs/papers/dwa_whitepaper_OrphanWorks.pdf (2014. szeptember 5.)
12. ECDLweb: A számítógép működési elve. In: ECDLweb, 2010. http://ecdweb.hu/A_sz%C3%A1m%C3%ADt%C3%B3g%C3%A9p_m%C5%B1k%C3%B6d%C3%A9si_elve (2015. március 10.)
13. IANNELLA, Renato: Digital Rights Management (DRM) Architectures =D-Lib Magazine, 7. évf. 6. sz. 2001. <http://www.dlib.org/dlib/june01/iannella/06iannella.html> (2015. június 15.)
14. Intertrust: Marlin Broadband Architecture Overview. Sunnyvale, 2011. <http://www.marlin-community.com/public/MarlinBroadbandArchitectureOverview.pdf> (2015. június 15.)
15. Intertrust: Marlin Tutorial. Sunnyvale, 2012. <http://www.marlin-community.com/files/MarlinTutorial2012.pdf> (2015. június 15.)
16. KANTARCIOGLU, Murat: Advanced Encryption Standard. The University of Texas at Dallas, Richardson, 2008. http://www.utdallas.edu/~muratk/courses/crypto09s_files/aes.pdf (2014. október 22.)
17. KAR, Saroj: A Look At SiDiM: A thought for e-book DRM to stop piracy. SiliconANGLE.com, 2013. 08. 19. <http://siliconangle.com/blog/2013/08/19/a-look-at-sidim-a-thought-for-e-book-drm-to-stop-piracy> (2014. augusztus 15.)
18. MAHMOUD-AREF-ABBADI, Imad: Digital Rights Management for Personal Networks. University of London, London, 2008. [doktori disszertáció] <http://digirep.rhul.ac.uk/items/231c27e9-a35c-9f96-36fd-25e4a2b9315b/1/RHUL-MA-2008-17.pdf> (2014. július 26.)
19. MOLDOVÁN István: E-könyvek, e-szövegek, könyvtárak =Könyv és Nevelés, 2014. 16. évf. 3. sz. http://olvasas.opkm.hu/portal/felso_menusor/konyv_es_neveles/ekonyvek_eszovegek_konyvtarak (2015. március 5.)
20. OTT, Matthias-Christian: Digital Rights Management. Universität Leipzig, Leipzig, 2010. <http://www.informatik.uni-leipzig.de/~graebe/Texte/Ott-10.pdf> (2014. július 25.)
21. PERRIN, Chad: Hacker vs. Cracker =TechRepublic, 2009. 04. 17. <http://www.techrepublic.com/blog/it-security/hacker-vs-cracker>
22. QIANG, Hao: E-book Security: An Analysis of Current Protection Systems. Linköping University, Linköping, 2003.

[doktori disszertáció] <http://liu.diva-portal.org/smash/get/diva2:19203/FULLTEXT01.pdf> (2014. július 20.)

23. Reuters: Marlin Community Announces Availability of eBook DRM Specification = Reuters Online, 2011. 08. 29. <http://www.reuters.com/article/2011/08/29/idUS142116+29-Aug-2011+BW20110829> (2014. augusztus 30.)
24. ROTHMAN, David: Barnes & Noble adopts open EPUB eBook Format, PDF and Adobe Content Server. TeleRead.com, 2009. 09. 20. <http://www.teleread.com/ebooks/barnes-noble-adopts-open-epub-ebook-format-pdf-and-adobe-content-server> (2014. augusztus 30.)
25. SCHULTZ, Rod: The many facades of DRM. 2012. http://www.whiteboxcrypto.com/files/2012_MISC_DRM.pdf (2014. július 26.)
26. SiDiM: SiDiM – Sichere Dokumente durch individuelle Markierung. 2011. https://www.sit.fraunhofer.de/fileadmin/dokumente/Projektblaetter/SiDiM_de.pdf (2014. augusztus 15.)
27. STALLMAN, Richard: Some confusing or loaded words and phrases that are worth avoiding. 2003. <http://www.gnu.org/philosophy/words-to-avoid.html> (2014. július 25.)
28. TORRES-PADROSA, Víctor: Contribution to an architecture for multimedia information management and protection based on open standards. Universitat Pompeu Fabra, Barcelona, 2008. [doktori disszertáció] <http://www.tdx.cat/bitstream/handle/10803/7547/tvtp.pdf;jsessionid=FEA5C976E256FB63618D184678B73CAD.tdx2?sequence=1> (2014. augusztus 12.)
29. TÓSZEGI Zsuzsanna: A szerzői jogok védelmét szolgáló digitális technológia = Tudományos és Műszaki Tájékoztatás, 2006. (53. évf.) 10. sz. 447–456. old. http://tmt.omikk.bme.hu/show_news.html?id=4533&issue_id=476 (2014. szeptember 27.)
30. VAN DE POL, Huub: BooXtream Usage Scenarios. 2014. [ügyfeleknek szánt nem publikus dokumentum]
31. VAN DE POL, Huub: eBook watermarking and personalisation distribution platform. 2014. [ügyfeleknek szánt nem publikus dokumentum]
32. VAN DE POL, Huub: Pricing BooXtream™ Web Service. 2014. [ügyfeleknek szánt nem publikus dokumentum]
33. ZHANG, Xiao: A Survey of Digital Rights Management Technologies. University of Washington, St. Louis, 2011. <http://www.cse.wustl.edu/~jain/cse571-11/ftp/drm.pdf> (2014. július 25.)

Jegyzetek

1. STALLMAN, Richard: Some Confusing or Loaded Words and Phrases that are Worth Avoiding. 2003. <http://www.gnu.org/philosophy/words-to-avoid.html> (Letöltve: 2014. július 25.)
2. TÓSZEGI Zsuzsanna: A szerzői jogok védelmét szolgáló digitális technológia = Tudományos és Műszaki Tájékoztatás, 2006. (53. évf.) 10. sz. 447–456. old. http://tmt.omikk.bme.hu/show_news.html?id=4533&issue_id=476 (2014. szeptember 27.)
3. AUSDERAU, Patrick: Protection mechanisms for electronic books. Helsinki Metropolia University of Applied Sciences, Helsinki, 2014. [doktori disszertáció] https://www.theseus.fi/xmlui/bitstream/handle/10024/74667/Ausderau_Patrick.pdf (2014. július 21.)
4. TÓSZEGI Zsuzsanna: A szerzői jogok védelmét szolgáló digitális technológia = Tudományos és Műszaki Tájékoztatás, 2006. (53. évf.) 10. sz. 447–456. old. http://tmt.omikk.bme.hu/show_news.html?id=4533&issue_id=476 (2014. szeptember 27.)
5. TÓSZEGI Zsuzsanna: A szerzői jogok védelmét szolgáló digitális technológia = Tudományos és Műszaki Tájékoztatás, 2006. (53. évf.) 10. sz. 447–456. old. http://tmt.omikk.bme.hu/show_news.html?id=4533&issue_id=476 (2014. szeptember 27.)
6. DEMARCO, Amanda: BooXtream on „social DRM” as a better option for e-books. 2012. <http://publishingperspectives.com/2012/09/booxstream-on-social-drm-as-a-better-option-for-e-books> (2014. október 25.)
7. TÓSZEGI Zsuzsanna: A szerzői jogok védelmét szolgáló digitális technológia = Tudományos és Műszaki Tájékoztatás, 2006. (53. évf.) 10. sz. 447–456. old. http://tmt.omikk.bme.hu/show_news.html?id=4533&issue_id=476 (2014. szeptember 27.)
8. http://beesbuzz.biz/blog/e/2010/01/07-interesting_topaz_drm_development.php (Utoljára megnyitva: 2014. december 10.)
9. BODÓ Balázs: A DRM-mítosz - mire jó és mire nem a másolásvédelem = Könyvmarketing konferencia, Budapest, 2010. <https://prezi.com/ecqe-mxidnuz/konyvmarketing-2010> (2014. december 7.)
10. <http://www.businessinsider.com/netflix-has-passed-hbo-in-paid-subscribers-2013-10> (2014. december 10.)
11. <http://fortune.com/company/NFLX/> (2014. december 10.)
12. <http://www.billboard.com/biz/articles/news/digital-and-mobile/6092226/spotify-now-has-10-million-paid-subscribers-3-million> (2014. december 10.)

Beérkezett: 2015. június 15.