



OCHRANA PROTI KOPIROVÁNÍ: Boj bez hranic

Stát a zábavní průmysl chtějí za každou cenu co nejlepší ochranu proti kopírování. Jako obvykle je to zákazník, kdo bude muset nést následky.

MARKUS MANDAU

Válka mezi hollywoodskými studií, hudebním průmyslem, vydavateli a piráty už trvá řadu let. Čas od času se podaří firmám a institucím piráty porazit, obvykle však tahají za kratší konec. Místo aby si ale uvědomily nesmyslnost tohoto boje a vyzkoušely nové taktiky a způsoby prodeje, pokouší se vymyslet stále lepší a lepší protipirátské ochrany. Ty pochopitelně prolomí během několika dnů, následky jejich nasazení však obvykle nese zákazník – nejčastěji v podobě omezeného použití nosiče. A bude hůř: podíváte-li se na aktuální návrhy amerických politiků a na nejnovější projekty zábavního průmyslu, zjistíte, že v budoucnu bude mít potenciální zákazník na výběr pouze mezi ztrátou soukromí a omezenými možnostmi využívání nosiče. Pokud bude mít navíc nakupující smůlu, může se dostat přímo do zuřící kybernetické války.

Dlouhou dobu byla kybernetická válka pouze záležitostí profesionálních hackerů, kteří se vydali na cestu do počítačů zahraničních vlád nebo kradli nové technologie z firemních sítí. Podle utajovaných informací nedávno zveřejněných Edwardem Snowdenem se kybernetické války (pravděpodobně při americké iniciativě) brzy objeví i na našem prahu – třeba i v podobě vylepšené ochrany proti kopírování filmů, hudby, knih, softwaru a her. Prvním krokem na této cestě je patrně zpráva komise Kongresu USA o krádežích amerického intelektuálního vlastnictví, která byla zveřejněna na konci května. Tato komise, jejímiž členy jsou vlivní politikové, specialisté v oboru a také státní úředníci, zkoumala důsledky krádeží duševního vlastnictví pro domácí ekonomiku a došla k odhadu škod ve výši více než 300 miliard dolarů ročně. Samotná zpráva se zaměřuje na tzv. čínský problém – od útoků profesionálních hackerů přes pirátskou výrobu značkové-

ho zboží v masovém měřítku až po porušování autorských práv prostřednictvím pirátských kopií filmů, hudby a knih.

Pokud jde o tvorbu ochranných mechanismů, nejprve zpráva shrnuje situaci, ve které se nachází běžní kupující, uživatelé online sdílených souborů a datoví piráti. Dále odborníci připravili několik návrhů, jak by měl v budoucnu průmysl a stát lépe chránit duševní vlastnictví. Jde jak o souhrn již existujících a používaných metod (například vodoznaky), tak i návrh na poněkud drastická opatření, která mohou způsobit přímé poškození dat. Za zmínku stojí například speciální software, který blokuje počítač piráta a zobrazí zprávu s názvem orgánu činného v trestním řízení, kde je potřeba se ke zrušení blokace zaregistrovat.

Ve zprávě je popsán i vládní trojský kůň, který při porušování autorských práv udělá z vašeho počítače rukojmí – podobně jako to v současnosti provádí malware označovaný jako ransomware. Další návrhy pro americkou legislativu pochází přímo z hackerské noční můry – například zjišťování totožnosti pachatele přes webovou kameru.

Návrat rootkitů

Cílem těchto opatření je zastavit ve velkém měřítku probíhající mezinárodní pirátství. Nikdo ale nezmiňuje vedlejší škody, které vtáhnou běžné internetové surfaře a poctivě nakupující uživatele chráněných médií do kybernetické války a pod palbu internetové mafie. Je totiž logické, že většina výše uvedených strategií vyžaduje pomoc z vnitřku počítače – obvykle v podobě trojského koně, který využije slabinu v operačním systému a zkontroluje vám počítač. A zmiňovaný trojský kůň se do počítače dostane nejčastěji z médií, na kterých si chráněný obsah zakoupíte. Přesně to před několika lety předvedla firma Sony, která svůj rootkit umístila na audio CD. Touto taktikou se inspirovaly další firmy a během krátké doby jste na rootkity mohli narazit například i u herních DVD.

Velmi brzy si však této taktiky všimli i počítačoví zločinci a začali masově využívat jak zranitelnost umožňující propašovat rootkit do počítače, tak později i služby samotného rootkitu. Například nedlouho po objevení rootkitu od Sony byl objeven i malware, který využíval služeb rootkitu pro maskování vlastní činnosti.

Systém CAS „šesti prohřešků“ (Six strikes) je v USA aktivní od února tohoto roku. Po šesti prohřešcích v podobě nelegálního stahování se uživateli sníží rychlost stahování na minimum.



Zažili jsme to již před šesti roky: disky chráněné rootkity. Pokud ale američtí experti prosadí své návrhy, čeká nás podobná ochrana i v budoucnu.

Jak se bude situace v budoucnu vyvíjet, stále není jasné, faktem ale je, že zatímco v USA jsou už nyní surfaři (a tedy potenciální piráti) masivně sledováni, evropská legislativa si na podobnou aktivitu zatím jen chystá zbraně. Pravděpodobně nejdále je Francie, která ale se svým zákonem „tříkrát a dost“ (známým také pod zkratkou HADOPI) narazila. Skupina expertů zjistila, že systém prosazující po třech porušeních zákona odpojení od internetu zcela selhal. Od letošního podzimu tak bude pouze nahrazen systémem pokut, který by měl viníky trestat efektivněji. Zpozornět by také měli uživatelé ve Velké Británii, kde ministr zahraničí letos v létě přiznal, že vláda monitoruje internet. Pokud jste prý ale zákonů dbalí občané, nemáte se čeho obávat. Česká republika má zatím díky svému poměrně unikátnímu zákonu povolujícímu určité stahování pro vlastní potřebu (více viz například → **Chip 1/2013, str. 28**) unikátní postavení, je ale jen otázkou času, než bude pod tlakem korporací tento zákon změněn a surfaři vystaveni důkladnému sledování.

P2P sítě: Nejen trn v oku

P2P sítě patří mezi nejmasivnější mechanismy umožňující výměnu dat, a to převážně v podobě autorským zákonem chráněného obsahu. A zajímavé je, že i přes neustálé postihy jsou nepřetržitě na vzestupu. Například tři největší světové trackery rozšiřují měsíčně v průměru 4,5 milionu souborů pro více než 30 milionů uživatelů.

Pokusem o reakci na tento trend je Copyright Alert System (CAS), který v USA působí od února. Jeho provoz byl zahájen v Centru pro informace o autorských právech (CCI) a podílí se na něm jak organizace chránící práva z oblasti hudby a filmového průmyslu, tak i například všichni velcí američtí poskytovatelé (například Comcast, Verizon a AT & T). CAS je postaven na principu dělby práce: firmy specializované na sledování peer2peer sítí najdou chráněný obsah a získají jménem držitele práva a zároveň i IP adresy zúčastněných uživatelů. Ty jsou předány příslušným poskytovatelům, kteří zajistí zobrazení varování na uživatelské počítači. V závislosti na velikosti prohřešku a provozovateli je připraveno až šest různých varování v podobě zpráv, které nelze vypnout. V případě, že na ně uživatel nereaguje, je možné omezit přístup k internetu až na rychlost 56 kb/s.

Zásadním problémem prý v současnosti je, že poskytovatelé nemohou snadno analyzovat datový provoz. Nedávno ale firma AT & T požádala o patenty, které by poskytovatelům umožňovaly sledovat P2P komunikaci ve své síti. Podle nejnovější zprávy už firma Comcast, největší poskytovatel kabelového vysílání v USA, stejně jako filmový a televizní producent NBC Universal, pracuje na jeho zavádění. Díky tomuto systému by bylo možné vystopovat uživatele během stahování, zablokovat ho a přesměrovat na stránku, kde si může zakoupit film legálně. To by mělo být efektivnější a především méně nákladné než současný stav, při kterém jsou pirátům masově rozepisovány varovné zprávy, případně následují soudní procesy.

Zvýšený uživatelský monitoring nepřímo znamená, že zábavní průmysl považuje další ochranné mechanismy za neúspěšné. A skutečností je, že například i dlouho vyvíjené šifrování AACs, používané například na Blu-ray discích, nepředstavuje ani pro amatérské piráty žádný problém. Stačí si jen nainstalovat software, jako například DVDFab nebo AnyDVD, a zkopírovat obsah Blu-ray nosiče v nešifrované podobě na pevný disk. Pro zkušenější piráty nejsou problémem dokonce ani DRM chráněné datové streamy, které jsou masově nahrávány na P2P portály nebo na weby hostingových služeb. Například jednotlivé části seriálu House of Cards, který produkovala firma Netflix, specializující se na streamování filmů, byly k dispozici ke stažení během jediného týdne. V tomto případě ale piráti neobešli DRM ochranu, ale chráněný obsah byl zaznamenán pomocí snímání obrazu.

Vodoznaky chrání obsah

Zatímco na první pohled komplikované šifrování proti pirátství téměř žádnou ochranu neposkytuje, jiná, zdánlivě jednoduchá metoda se ukázala jako účinná. Tou je vodoznak označovaný jako Cinavia, kterým jsou od roku 2010 (kromě šifrování AACs) chráněny Blu-ray disky. Ačkoliv profesionální piráti tuto ochranu pravděpodobně odstranit dokážou, masově rozšířené nástroje si s ní doposud neporadí.

Nejprve tuto ochranu začala používat společnost Sony Pictures, postupně se však začala připojovat i další filmová studia. Na podrobnější rozebrání principu této ochrany zde není prostor, zajímavé je ale její fungování v praxi: pokud BD pře-



VSTŘÍCNOST K ZÁKAZNÍKOVÍ: LEGÁLNÍ NÁKUP A PIRÁTSTVÍ

Charakteristickým rysem současných ochranných a protipirátských opatření je minimální účinnost proti pirátům a výrazná nepřátelskost vůči legálním nakupujícím. Typickým příkladem může být například nákup filmu na DVD.



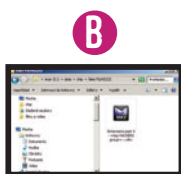
A NÁKUP DVD V OBCHODU

1. Spustí film v DVD přehrávači.
2. Sleduje přibližně minutové anti-pirátské video „auto byste neukradli...“
3. Čte textové upozornění varující před pirátským.
4. Sleduje film.



B PIRÁT

1. Stáhne film a klikne na soubor.
2. Sleduje film.



NEÚČINNÝ

Teprve nedávno nasazená ale už prolomená: Pirátské kopie filmu Nespoutaný Django se na internetu objevily už v květnu, navzdory ochraně Cinavia.

1. Nespoutaný Django
2. Hobbit: Neočekávaná cesta
3. G.I. Joe: Odveta
4. Mocný vládce Oz
5. Z cizího krev neteče

PLACENÁ INZERCE

hrávač detekuje Cinavii, ale bez ochrany proti kopírování, pravděpodobně se jedná o nelegální kopie. Co se bude dít dál, to závisí na implementaci kódu Cinavia. V některých přehrávačích se objeví hlášení:

Playback stopped. The content being played is protected by Cinavia and is not authorized for playback on this device. For more information see www.cinavia.com.message code1.

Někdy ještě film hraje asi 20 minut, ale s vypnutým zvukem. Na obrazovce se poté objeví zpráva „Zvuk vypnutý, protože mediální obsah, který chcete přehrát, nemá oprávnění pro přehrávání na tomto přístroji“. Zajímavé je, že tento vodoznak chrání i před přehráním filmů nelegálně nahraných například kamerou v kině – přehrávač zastaví přehrávání a okamžitě se zobrazí příslušné hlášení.

Lobby majitelů autorských práv prosadila, že od února 2012 je detekce Cinavie povinná ve všech nových Blu-ray přehrávačích. To překvapivě platí i pro softwarové přehrávače, jako jsou PowerDVD nebo TotalMedia Theatre. Jako největší zastávce této ochrany vložila firma Sony Cinavii prostřednictvím aktualizace firmwaru dokonce i do některých svých starších modelů přehrávačů (včetně herní konzole PS3). Zajímavé ale je, že přehrávače multimédií v nejnovějších televizorech a také počítačových operačních systémech vodoznak nedetekují a filmy přehrávají bez jakýchkoli problémů.

Cinavia přežije konverze?

Vzhledem k tomu, že Cinavia je ochrana související s audiostopou, teoreticky ji lze odstranit pomocí editoru, jako je například freeware Audacity. Faktem ale je, že po odstranění ochrany se ve všech verzích, které jsou v oběhu na internetu, výrazně snižuje kvalita zvuku.

V současné době pracují na vhodném řešení tvůrci kopírovačícího softwaru DVD-Ranger. Podrobně zkoumají, jak Cinavia mění zvukovou stopu: vedle vodoznaku se také od původního zvuku liší rychlost přehrávání. To vede k mírným audiovýkyvům, které mohou dobře trénované uši odhalit. Nicméně tyto výkyvy jsou součástí ochrany proti kopírování, protože bez těchto změn by bylo možné snadno odstranit vodoznak porovnáním zdroje

zvuku s formátem, ve kterém byl vydán film (například 5.1 zvuku na DVD), který nemá ochranu Cinavia.

Druhá část vodoznaku je umělý signálový šum, který je realizován v celém filmu prostřednictvím modulace o frekvenci mezi 400 a 4 000 Hz. Tento hluk ale lidské ucho může slyšet. Aby se tomu zabránilo, mění se jeho síla pomocí psychoakustického filtru takovým způsobem, že ho lidské ucho nerozpozná. Využití tohoto frekvenčního rozsahu vede k tomu, že pokud se někdo tuto ochranu pokusí odstranit, objeví se v nahrávce značný hluk na pozadí.

CinEx plug-in pro DVD-Ranger je sice stále v beta-verzi, ale i po několika měsících vývoje se při odstraňování ochrany Cinavia i nadále podstatně snižuje kvalita zvuku. To je důvod, proč v současné době software stále ještě nelze použít.

Jinou cestou šla firma SlySoft se svým AnyDVD. Verze 7.3.1.0, která byla zveřejněna v srpnu, deaktivuje ochranu Cinavia v rámci softwarového přehrávače. Zeptali jsme se společnosti SlySoft, jak se jí to povedlo, ta ale odmítla odhalit technické detaily. Pouze zdůraznila, že jí trvalo dlouhou dobu, než dosáhla slušných výsledků. Lze jen spekulovat, zda vývojáři SlySoftu nějakým způsobem deaktivovali programovou knihovnu přehrávače relevantní pro Cinavii, nebo zda Cinavii zmanipulovali jiným způsobem.

V každém případě lze říci, že v budoucnu se podaří prolomit i tuto ochranu v plném rozsahu a že je jen otázkou času, než se objeví jednoduché nástroje na kopírování obsahu Blu-ray disků. Vlastníci autorsky chráněného multimediálního obsahu tak brzy budou nuceni poohlédnout se po nových metodách ochrany – nebo jít s dobou a problém s piráty vyřešit jiným způsobem.

Další na řadě: E-knihy

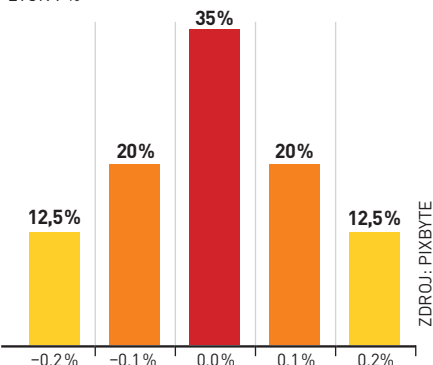
K podobné situaci jako u multimediálních dat dojde brzy i u e-knih – elektronických verzí klasických knih. S jejich stále rostoucí oblibou a rozšířením bude docházet k překonávání stávajících ochrany a pravděpodobně i k vymyšlení lepších metod, jak zabránit masivnímu kopírování chráněného obsahu.

V současnosti jsou elektronické knihy distribuovány především ve dvou formátech: mobi pro čtečky Amazon Kindle a epub. Oba formáty nabízí možnost ochrany DRM, odstranit ji

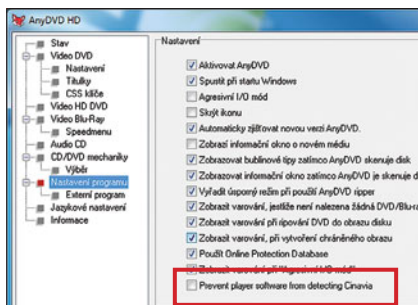
VODOZNAK CINAVIA CHRÁNÍ BLU-RAY A FILMY

Ochrana Cinavia je vložena jako další signál do zvukové stopy. Tak by teoreticky mohla být odstraněna (nebo blokována) na úkor kvality zvuku. I přesto jsou již k dispozici pirátské verze filmů s touto ochranou.

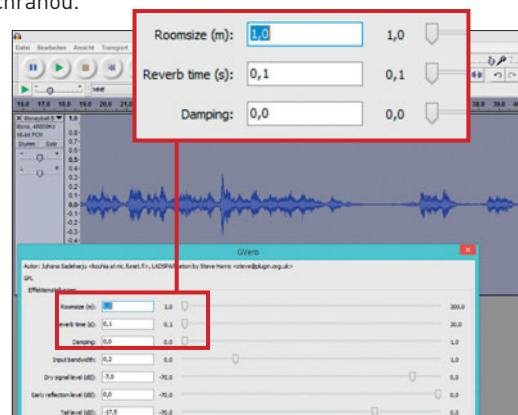
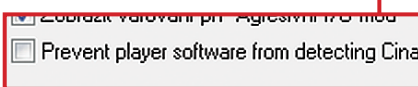
ODCHYLKA OD RYCHLOSTI ORIGINÁLU ZVUKU V %



Ochrana Cinavia nelze odstranit pomocí srovnání s původním zvukem: zvuk je míchán neustále se měnící rychlostí.



Nástroj AnyDVD nyní umožňuje deaktivaci Cinavia přímo v softwarovém přehrávači



Řešení v podobě odstranění ochrany Cinavia pomocí audio editoru jako například Audacity již existuje, ale kvalita zvuku je značně zhoršená.

PLACENÁ INZERCE

ale není ani pro méně zkušené uživatele problém. Stačí jen do oblíbeného nástroje pro konverzi a organizování knih jménem Calibre přidat jednoduchý doplněk, který vám DRM (u vámi zakoupené knihy) odstraní při importu knihy. Jedinou podmínkou je, že člověk musí nejprve e-knihy zakoupit a mít klíče k dispozici v počítači. Možná se ptáte, proč vlastně tuto ochranu odstraňovat, ale důvod je překvapivě prostý. Jednotlivé ochrany bohužel nejsou kompatibilní, a tak pokud jste si nakoupili knihy ve formátu epub a nyní máte čtečku od Amazonu, tyto knihy si na ní nepřečtete.

Je ale nutné zmínit, že Česká republika má v této oblasti překvapivě unikát. Někteří domácí vydavatelé si uvědomili, že cesta přes stále obtížnější a složitější ochrany nevede – kdo si někdy zařizoval Adobe ID s programem Adobe Digital Editions (pouze v angličtině), určitě ví, o čem mluvíme.

Domácí vydavatelé ale sází na vstřícnější ochranu označovanou jako sociální DRM. V praxi to znamená, že do knihy je na začátek (případně do zápatí) vložen například text: Zakoupil Jiří Novák, Jedlová 5845, Praha. Výhodou této „ochrany“ je skutečnost, že knihu můžete přečíst v libovolné čtečce bez jakýchkoliv omezení. Přidaný text pochopitelně není obtížné odstranit, většina uživatelů ale chápe, že jde o férovou dohodu mezi vydavatelem a čtenářem: vydavatel nehází čtenáři pod nohy klacky v podobě bizarních ochranných a omezení, čtenář knihu dále nešíří na internetu.

Kupujícího identifikuje SiDiM

Podobný rozumný přístup však většina zahraničních vydavatelství nemá, a tak není žádným překvapením, že se například v sousedním Německu začíná vyvíjet nový typ ochrany. Lokální knihkupci ve spolupráci s Fraunhoferovým ústavem pro bezpečnost informačních technologií a s dalšími partnery z vydavatelství připravují nový „vodoznak“ pro ochranu knih. Tato technologie, označovaná jako SiDiM (Secure Documents through Individual Marking), má kopírování e-knih zabránit prostřednictvím zastrašování. U e-knih to ale mají (na rozdíl například od multimediálních souborů) ochránci práv mnohem těžší – jednotlivá zařízení (čtečky) se od sebe často rapidně liší a i kvůli masové výrobě v Asii je takřka nemožné výrobce donutit k detekci ochranných mechanismů. Dalším problémem také je, že principiálně je většina knih prodávána ve formátu,



„Změny v obsahu knihy by pro čtenáře neměly být nepříjemné“

DR. ING. MARTIN STEINEBACH,
Fraunhofer Institut, projektový
manažer ochrany SiDiM


který je tvořen HTML konstrukcí s jednoduchým formátováním a který neponechává téměř žádný prostor pro další informace v podobě vodoznaku. SiDiM na to jde tedy jiným způsobem – zakoupenou knihu upraví tak, aby ji (v případě pirátského rozšíření) bylo možné vysledovat až k původnímu majiteli.

Princip SiDiM spočívá v tom, že jsou v každé knize automaticky provedeny drobné (ale viditelné) úpravy textu – například záměna synonym. Dalo by se tak říci, že kupující vlastně nedostane od autora originální knihu, ale její téměř identickou kopii.

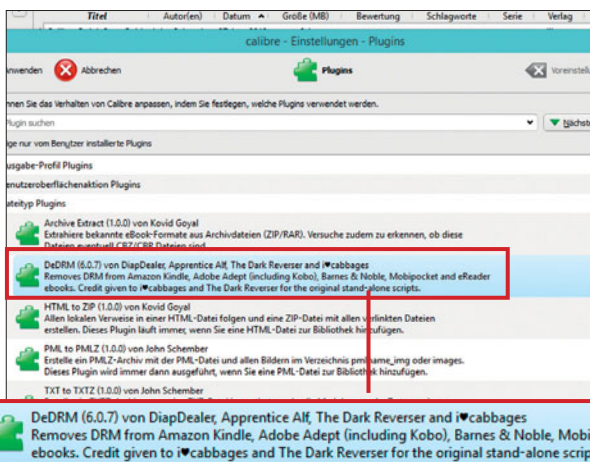
Také je důležité zdůraznit, že počet změn potřebných pro získání jednoho vodoznaku (jednoznačně identifikujícího knihu) závisí na očekávaných prodejkách. Čím vyšší je náklad, tím více úprav je nutné v knize udělat: například na 1 000 prodaných e-knih musí software SiDiM změnit maximálně deset částí textu. A pokud by chtěl pirát SiDiM odstranit, musel by mít k dispozici originál a vlastní knihu s ním porovnat.

Tato ochrana ale vyvolala v literárních kruzích hotový poprask: většina reakcí se pohybuje od výrazu „bizarní“ až po „neuvěřitelnou drzost vůči autorům“.

I přesto v současné době probíhá pilotní projekt, v rámci kterého jsou na webu umístěny texty ukazující SiDiM v praxi. Samotný software pro SiDiM už je ale připraven pro praktické nasazení a čeká pouze na závěrečné hodnocení účastníky projektu a zájem ze strany vydavatelství. V blízké budoucnosti se tedy ukáže, zda originál knihy zůstane vyhrazen pro papírovou verzi a ve svých čtečkách budeme číst pouze upravené kopie.

Při pohledu na všechny ty plány a projekty, které jsou připraveny nebo čekají na svou realizaci, je jasné, že v budoucnu budou mít kupující digitálních médií jen příslovečný výběr mezi větším a menším zlem. 

AUTOR@CHIP.CZ



Aus: Sigmund Freud - Eine Kindheits Erinnerung aus Dichtung und Wahrheit

Text 8

Das Hinausbefördern (durchs Fenster auf die Straße) erweist sich so als das Wesentliche der Handlung, die Lust am Zerbrechen, am Klirren und die Art der Dinge, an denen »die Exekution vollzogen wird«, als inkonstant und unwesentlich.	Das Hinausbefördern (durchs Fenster auf die Straße) erweist sich so als das Wesentliche der Handlung, die Lust am Zerbrechen, am Klirren und die Art der Dinge, an denen »die Exekution vollzogen wird«, als konstant und unwesentlich.
Linker Text wurde modifiziert	Rechter Text wurde modifiziert
Sehr störend	Sehr störend
Störend	Störend
Leicht störend	Leicht störend
Nicht störend	Nicht störend
Nicht unterscheidbar	Nicht unterscheidbar
Nicht störend	Nicht störend
Leicht störend	Leicht störend
Störend	Störend
Sehr störend	Sehr störend

Německý protipirátský vynález:
V rámci testu se zkouší, jak moc bude čtenářům vadit modifikace originálního textu. Pokud se SiDiM osvědčí, nasadí ho v praxi i vydavatelé.

DRM z e-knihy lze automaticky odstranit pomocí doplňku pro bezplatný program sloužící ke konverzi a katalogizaci knih jménem Calibre.