Digital Rights Management

Když nejde zabránit kopírování, bude chráněn přímo obsah

MICHAL ILLAN A JAN NĚMEC

Co je to Digital Rights Management (DRM) a proč byl vyvinut? S rozvojem elektronických médií se objevil palčivý problém nelegálního kopírování a distribuce. Tento problém zahrnoval a stále zahrnuje především obsah v audio a video formátech – filmy a hudbu. Velmi brzy se přišlo na to, že kopírování a distribuci obsahu se nedá zabránit a že se stále se rozvíjející technologií se tento problém bude zhoršovat. Přibližně v této době se začal prosazovat zcela nový přístup. „Když není možné zabránit kopírování a distribuci, chraňme raději přímo obsah."

Historie

Jednou z prvních kvazi-DRM aplikací byla distribuce fontů. Na počátku devadesátých let byly fonty velmi drahé, ceny se pohybovaly ve stovkách dolarů (to bylo dříve, než Microsoft začal fonty ve velkém zdarma přidávat k Microsoft Office). Když byl soubor s fonty na síťovém serveru, bylo velmi snadné ho nelegálně zkopírovat. Na tuto situaci reagovali dva dodavatelé, InfoSafe a CDMax. Vyvinuli technologii, která umožňovala používat fonty šifrované na CD-ROM pouze po zadání dešifrovacího klíče.

Samotný začátek vývoje toho, čemu říkáme DRM systémy, proběhl v letech 1995–6. Vznikly dva komerční systémy. První byl InfoMarket z dílny IBM, který celý proces ochrany dat řešil softwarovou cestou. Druhý systém, založený na end-to-end hardwarovém řešení, vyvinula firma Electronic Publishing Resources (EPR). Ani jeden z uvedených systémů se však neprosadil. Část systému InfoMarket se později objevila v systému Electronic Media Management System (EMMS) firmy IBM. EPR později změnil svou technologii z hardwarové na softwarovou a přejmenoval se na InterTrust. Třetím důležitým zdrojem myšlenky DRM byla kniha Letting Loose the Light: Igniting Commerce in Electronic Publication, napsaná Dr. Markem Stefikem, vývojovým pracovníkem Xerox PARC Research Labs. V této knize byl popsán Digital Property Rights Language (DPRL), jazyk pro popis práv aplikovaných na chráněný obsah. Na jeho základě vyvinul Xerox technologii, kterou sice úspěšně otestoval, ale nepodařilo se mu ji prodat. Z divize Xerox Rights Management se později stala firma ContentGuard, která vytvořila Extensible Rights Markup Language (XrML), který se dnes stal technologickým standardem.

Po roce 1996 vzniklo (a v mnoha případech následně zkrachovalo) poměrně mnoho výrobců. Pozitivním příkladem je společnost Liquid Audio, která funguje od roku 1996 dodnes. Po celou dobu své existence se věnuje vývoji systému pro distribuci hudby přes internet.

Současně začínaly vznikat různé iniciativy ze strany distribučních společností a výrobců koncových zařízení. Příkladem je asociace DVD Copy Control Association s technologií Content Scramble System (CSS). U zrodu této technologie stála kolem roku 1996 Toshiba, Warner a Matsushita, později se přidali BMG, Sony a další. Samotné CCS kódování obrazu bylo úspěšně prolomeno v roce 1999. Dokonce byl na internetu distribuován program DeCCS, který umožňoval přehrávání DVD na systémech, které CCS nepodporovaly. Takzvané regionální kódování, které mělo zabraňovat přehrávání disků v jiných oblastech, než kam byly distribuovány, bylo a stále je sabotováno samotnými výrobci koncových zařízení.

K významnému rozvoji na poli DRM dochází až v tomto století. Období roku 2000 a 2001 je charakteristické další vlnou nových firem implementujících DRM technologie, rok 2002 pak charakterizují krachy a skupování těchto firem velkými investory. Například Sony a Philips Electronics se spojily k nákupu firmy InterTrust především z důvodu získání velkého množstvím klíčových technologických patentů.

V oblasti prodeje práv k obsahu prostřednictvím internetu působí především RealNetworks a Microsoft. Počátkem roku 2004 se zdá být hlavním hráčem Microsoft.

Na začátku roku 2003 bylo DRM řešení firmy RealNetworks nasazeno pouze na stránkách MusicNet.com, založených firmami BMG, EMI, Warner Brother a RealNetworks. RealNetworks posléze koupilo Listen.com a vyhlásilo, že bude převeden na jejich technologii z Microsoft DRM, což se také stalo. V březnu 2004 společnost Virgin překvapivě oznámila, že s MusicNet.com spolupracuje na službě „on-line music service" Virgin Digital, která by měla zpřístupňovat více než 700 000 zvukových záznamů ve formátu Windows Media.

Situace Windows Media DRM firmy Microsoft je odlišná. Už od roku 2001 se tato platforma postupně rozšiřuje, zahrnuje nové standardy, v roce 2004 přibyla podpora přenosných zařízení (portable devices). Windows Media 9 DRM je nasazeno například v nové verzi napster.com (v současné době spojené s PressPlay.com, založeno Universal Music, Sony Music a Microsoftem) a v Evropě v MSN Music Club a Tiscali Music Club Online, založenými Microsoftem a OD2. Není třeba se však obávat monopolu. V květnu 2004 spustilo Sony svůj vlastní DRM portál založený na vlastní technologii Open MagicGate (OpenMG) a formátu ATRAC. British Telecom oznámil spuštění vlastní služby BT Rich Media, která bude podporovat jak DRM firmy Microsoft, tak RealNetworks.

Další oblastí uplatnění DRM jsou tzv. eBooks. V této oblasti se už mnoho let kromě jiných prosazuje Adobe s PDF formátem.

Windows Media DRM

První funkční komerční DRM systém pro audio a video obsah byl Microsoftem vytvořen v roce 1999 (verze 1), v roce 2000 a 2001 vyšly verze 7 a 7.1. V této době je stále aktuální verze 9, uvolněná v roce 2003.

Základní myšlenkou Windows Media DRM je oddělení distribuce obsahu od distribuce práv k jeho užívání. Toho je dosaženo zašifrováním souboru s hudbou či videem a jeho distribucí v této formě. Uživatel se po stažení takového souboru z internetu nebo zkopírování od kamaráda pokusí soubor spustit ve Windows Media Playeru. Je upozorněn na to, že se jedná o chráněný soubor, a otevře se mu okno s www stránkou poskytovatele obsahu, kde si zakoupí licenci k přehrání. Po zakoupení a stažení licence je možné chráněný soubor spustit.

Celý proces se skládá z těchto kroků:

1. Šifrování – Soubor typu .wmv nebo .wma je zašifrován pomocí privátního klíče. Do souboru jsou přidány informace o verzi DRM, identifikaci obsahu a URL adresa odkazující na www stránku, kde je možné získat licenci. Hlavička souboru je podepsána tak, aby nebylo možné některé údaje změnit. V případě, že odkaz na www stranu distributora obsahu je například pozměněn, přehrávač to pozná a varuje uživatele.

2. Distribuce – Zašifrované soubory je možné distribuovat zcela volně přes internet, na CD, emailem nebo si soubor prostě zkopírovat od kamaráda.

3. Licence Clearing House – Poskytovatel obsahu se rozhodne pro nějaký existující Licence Clearing House nebo, jako v případě Českého Telecomu a jeho StarZone, ho implementuje. Mezi funkce Clearing House patří udržovat veškeré informace o vazbách mezi obsahem, právy, distributory a vlastníky obsahu. Další funkce zahrnují autentifikaci žádosti uživatele o licenci a ve spolupráci s licenčním serverem generování odpovídající licence.

4. Nákup licence – Aby koncový uživatel mohl chráněný soubor přehrát, musí nejdříve získat licenční klíč. Při pokusu o přehrání chráněného souboru Windows Media Player zkontroluje, zda má uživatel platnou licenci. Pokud licenci najde, soubor se začne automaticky přehrávat. V opačném případě se otevře okno s webovou stránkou distributora obsahu, kde si uživatel licenci zakoupí. Zakoupená licence je doručena na uživatelův počítač ve tvaru zašifrovaném pro konkrétní počítač (viz individualizace) a uložena. Licenci je možné doručit tzv. hlučně, kdy je uživatel o doručení informován, nebo tiše, kdy doručení proběhne na pozadí aplikace.

5. Přehrání – Windows Media Player zkontroluje licenci a dovolí chráněný soubor přehrát v souladu s obsahem licence. Licence samotná obsahuje soubor práv (viz práva) a nastavení, omezujících uživatelův přístup a manipulaci s obsahem. Součástí licence je také zašifrovaný veřejný klíč k chráněnému souboru.

Individualizace

Windows Media připojí ke každé instalaci Windows Media Playeru jednoznačnou identifikaci. To zabrání distribuci pozměněného playeru po internetu, protože je možné ho jednoznačně identifikovat a případně vyřadit z provozu v průběhu generování licencí.

Práva

Každá licence zahrnuje celý soubor omezení uživatelova přístupu k chráněnému souboru. Takto je možné omezit počet přehrání, dobu, po kterou je možné soubor přehrávat, datum, od kdy a do kdy je možné soubor přehrávat nebo například zda je možné obsah dále přenášet na přenosná zařízení.

Šifrování

Pro autentifikaci a výměnu klíčů jsou použity algoritmy Elliptic Curve, ECC-ElGamal a ECC-DSA, pro šifrování dat RC4 a DES. Samotný Microsoft je v této oblasti velmi mlčenlivý, protože utajení ochranných mechanizmů se ukázalo být zatím nejbezpečnější strategií ochrany proti hackerům.

Bezpečnost

V oblasti bezpečnosti poskytuje koncepce zajímavé funkce. Může to být například Secure Audio Path, kde Windows Media umožňují zajistit ochranu obsahu na úrovni operačního systému. To se týká především cesty z přehrávače do ovladače zvukové karty tak, aby nebylo možné proud dat zachytit uvnitř v počítači. Další možností je vyloučení aplikace (při vydávání licence je možné zakázat přehrávání v konkrétních aplikacích) či DRM komponenty (při generování licence je možné zakázat přehrávání v konkrétních DRM komponentách, o nichž je známo, že byly zkompromitovány).

Next Generation Windows Media DRM

V květnu Microsoft ohlásil novou verzi Windows Media DRM, která přinese nové možnosti jak na úrovni obchodních scénářů, tak i v rozšíření počtu podporovaných přenosných přehrávačů, mobilních telefonů a PDA. Nezbývá mi než s humorem dodat: „Pevně doufám, že až budete tento stručný popis základní koncepce Windows Media 9 DRM číst, nepůjde už o překonanou verzi."

První komerční DRM systém v České Republice

Prvním komerčně provozovaným systémem distribuce videa a hudby v České republice a ve střední a východní Evropě vůbec, založeným na technologii DRM, je portál StarZone (www.starzone.cz), který vybudoval a nedávno spustil Český Telecom. Projekt nasazení DRM jako komerční služby se začal připravovat již počátkem minulého roku. Nejtěžší bylo na počátku přesvědčit vlastníky obsahu, že celý systém DRM je dostatečně důvěryhodný a bezpečný. Poté, co se podařilo uzavřít dohodu s několika z nich, začala práce na implementaci. Pro implementaci DRM v České Republice vybral Český Telecom ve spolupráci s Logicou CMG systém DMDfusion firmy DMDSecure, což je průmyslové multiplatformní řešení, umožňující provozovat vedle sebe DRM technologii Microsoftu i RealNetworks. Toto řešení má formu „kostky" s otevřenými rozhraními, kterou je třeba následně integrovat do konkrétní infrastruktury provozovatele Clearing Housu.

Celý systém funguje poměrně jednoduše. Obsah – film nebo písnička – je převeden do digitální podoby (wmv) a do systému jsou zadána základní data, která ho popisují a jsou prezentována na webových stránkách. Poté je soubor zašifrován, jsou do něj přidány informace, které ho identifikují pro nákup licencí a je uložen pro stažení. Uživatel si na webových stránkách podle zobrazených informací, jako například ve videopůjčovně, vybere titul, který si chce prohlédnout, a stáhne soubor na svůj počítač, nebo, má-li dostatečné připojení, rovnou ho spustí. A už jen stačí vybrat si typ licence, autorizovat na automaticky otevřené webové stránce a sledovat vybraný film.

Nakonec jsme byli příjemně překvapeni pozitivní reakcí odborné veřejnosti. Věříme proto v budoucí rozšíření DRM technologie jako logického vyústění současného problému s nelegálním kopírováním audio a video obsahu.

Závěrem

Je velmi zajímavé v poslední době sledovat překotný rozvoj DRM technologie i konkrétních řešení. Do budoucna lze předpokládat další odklon od čistě hardwarových řešení. Paul Kocher, Joshua Jaffe, Benjamin Jun, Carter Laren a Nate Lawson z firmy Cryptography Research, Inc. se domnívají, že budoucnost DRM systémů spočívá v myšlence Self Protecting Content (obsah, který se chrání sám). Vlastní přehrávač by fungoval podobně jako interpreter nebo virtual machine (podobně jako Java) a samotný kód dekryptoru by byl součástí obsahu. V případě, že by byla šifra prolomena, stačilo by na nově distribuovaná DVD s filmy nebo do obsahu na internetu pouze přibalit vylepšenou verzi dekryptovacího programu. 4 0364/FEL ❑