Soumrak protikopírovací ochrany

Každé opatření, které má zabránit nedovolenému kopírování multimediálního obsahu, dnes hackeři prolomí – dokonce i u Blu-ray a HD-DVD. To nutí filmový a hudební průmysl k přehodnocení dosavadních postojů. Zřekne se nakonec DRM? *Markus Mandau, autor@chip.cz*

V tomto článku najdete

Koupit, kreknout, zkopírovat – proti tomuto „zhodnocovacímu“ postupu nejsou obrněna ani ta největší esa multimediálního průmyslu. Přesto však téměř každá webová hudební služba jako iTunes, Napster nebo Yahoo chrání své skladby pomocí DRM (Digital Rights Management) – jinak by totiž od hudebního průmyslu žádné další tituly nedostala. Ochranou proti kopírování je opatřen také každý kotouček s hollywoodským filmem – ať už jde o dávno kreknutý DVD, nebo o nové disky s vysokým rozlišením. Avšak dokonce i ochrana HD-DVD a Blu-ray už se pomalu stává historií.

Současný stav přináší neblahé důsledky: zákazníci, kteří protikopírovací ochranu respektují, potřebují přídavný hardware i software – zároveň však ke chráněnému médiu mají jen omezený přístup. Uživatelé, kteří to neakceptují, jsou tlačeni do ilegality. Přesto se však ve výměnných burzách masově šíří profesionálně zhotovené pirátské kopie. Tím hloupým je dnes vlastně jen ten, kdo si produkt poctivě zakoupil.

A proč tomu tak je? Ani geniální hackeři, ani lenivý průmysl, ani chamtiví piráti – nic z toho nekompromituje protikopírovací ochranu tolik jako starý dobrý PC. Moderní mechanismy DRM už se dnes neprolamují, nýbrž odposlouchávají, zatímco pécéčko počítá.

ON-LINE HUDBA

Neomezené stahování díky hackerům

Úspěšným hráčem v aréně internetového byznysu je iTunes Music Store: Apple je celosvětově na čtvrtém místě mezi všemi obchodníky s hudbou, tedy i těmi, kteří distribuují CD. V současnosti funguje na webu vedle Applu prakticky už jen DRM ochrana od Microsoftu, kterou používají všichni velcí konkurenti jako Napster nebo Musicload.

Průlom č. 1: Naivní Apple

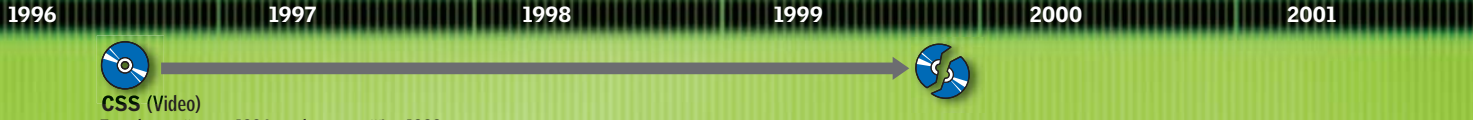
Apple svůj před čtyřmi lety zavedený model DRM pojmenoval „FairPlay“ – a jeho restrikce jsou skutečně natolik „fair“, že nikoho nezadrží: každá skladba získaná prostřednictvím iTunes se dá vypálit na nechráněný Audio CD.

Přesto si hackeři dali tu práci a DRM ochranu prolomili, čímž uživatelům ušetřili překódování, vždy zatížené ztrátami kvality. Norský hacker Jon Lech Johanssen „zboural“ FairPlay už v listopadu 2003. Jeho QTFairUse prostě ze songu od iTunes ukládá pouze zvuková data, čímž odstraňuje ochranu DRM. Apple sice mezitím FairPlay zdokonalil, avšak s QTFairUse6 pak v létě 2006 jiní hackeři applovský formát opět přelstili. A to platí až do současné verze iTunes 7.0.2.

Přitom je typické, že se hackerský software nijak nestará o zašifrování, ale prostě si „vyčíhá“ moment, kdy iTunes ukládá dešifrovanou skladbu frame po framu do operační paměti, aby ji poslal do zvukové karty. →

Protikopírovací ochrana: Pokaždé prolomena

Ať šlo o on-line hudbu, DVD Video, nebo o HD disky, vždy to dopadlo stejně: jejich ochrana proti kopírování byla prolomena, a to ve stále kratším čase.



CSS (Video)
Zavedena v červnu 1996, prolomena v říjnu 1999

Microsoft DRM 1 (Audio)
Zavedena v dubnu 1999, prolomena v říjnu 2001

→ Průlom č. 2: Bezmocný Microsoft

V srpnu 2006 si Microsoft se svou protikopírovací ochranou prožil malé peklo. Jistý hacker, který si říká „viodentia“, uveřejnil nástroj FairUse4WM, jímž může každý, kdo si zakoupil chráněný song, odstranit DRM od Microsoftu („PlaysForSure“). Hackerovou motivací byla ctižádost „poměřit se s tržním lídrem“. Přitom také odhalil, že Microsoft nedbal ani na aplikaci „jednoduchých bezpečnostních rutin“. A tak například Media Player ve verzích 10 a 11 beta si 56bitový klíč v otevřeném tvaru ukládá do operační paměti, odkud může být extrahován. Jakmile přehrávač začne chráněnou skladbu reprodukovat, hackerský program si ihned klíč načte. A právě s tímto klíčem odstraní nástroj jakékoliv omezení předepsané DRM. To všechno probíhá stejně rychle jako normální proces kopírování.

Zvláště tvrdě to postihne abonenční služby jako Napster. Tento portál umožňuje neomezené stahování skladeb za 10 USD měsíčně. Jejich DRM je limituje na 30 dnů – pokud ovšem uživatel nemá FairUse4WM. Takový zákazník by se mohl u Napsteru přihlásit, po celé dny nepřetržitě „nasávat“ písničky a pak je dešifrovat. Žádnou abonenci už pak nepotřebuje...

Neúčinná záplata: Po dvou neúspěšných úpravách DRM zveřejnil Microsoft finální verzi Media Playeru 11, s nímž už FairUse4WM nefunguje. Poněvadž však uživatele Windows k updatu na verzi 11 nic nenutí, hackerský nástroj se dá používat i nadále.

Oznámení na neznámého pachatele: Mezitím se Microsoft pokouší dostat pachatele před soud. Jak tvrdí právní zástupkyně Microsoftu Bonnie MacNaughtonová, viodentia „k napsání svého nástroje zcizil kód Microsoftu“. Hackerova odpověď vyzněla v tom smyslu, že zdrojový kód vůbec nepotřeboval, Microsoftem používané knihovny s šifrovacími algoritmy jsou veřejné a může je využít každý. Na celém postupu by nic nezměnily ani záplaty. Ty by snad mohly jen krátkodobě ztížit vyhledání správného místa v RAM. Tolik viodentia ve svém až dosud posledním „veřejném“ vyjádření na jednom internetovém fóru.

Steve Jobs: DRM musí pryč

Koncepci DRM však už zpochybňují i samotní zástupci hudebního průmyslu. Například společnost EMI oznámila, že napříště bude na webu distribuovat nechráněné skladby. Také Dave Goldberg, šéf Yahoo Music, předpokládá, že do konce roku už bude DRM patřit historii. A dokonce i „guru“ Applu Steve Jobs nahlas přemýšlí o zrušení DRM. Má k tomu pádný argument: Co je platné chránit on-line média, když 90 % prodané hudby jde v podobě Audio CD přes pulty obchodů? Jejich ochrana proti kopírování se už několik let jeví jako neefektivní, a odtamtud pocházejí ilegální MP3.

HD-DVD & BLU-RAY

Možná rekord: Prolomená ochrana už při uvedení na trh

Ještě nikdy nebylo věnováno protikopírovací ochraně tolik úsilí: filmová data na Blu-ray a HD-DVD jsou vždy zašifrována, ať už přímo na disku, v počítači, nebo na cestě z grafické karty do monitoru. Samotný film chrání AACS, cestu hardwarovými komponentami zabezpečuje protikopírovací ochrana zvaná HDCP.

Průlom č. 1: Děravé přehrávače

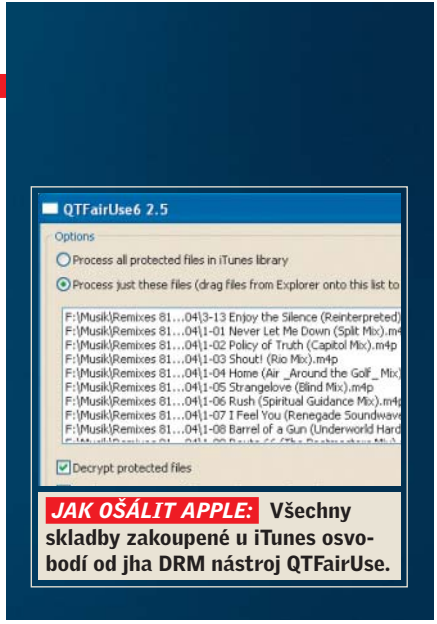
Pro uživatele PC to znamená především nepříjemnosti a další náklady: potřebuje grafickou kartu kompatibilní s HDCP, právě takový monitor a silný počítač. Všechny výdaje kvůli HDCP by ovšem neměly smysl, pokud by byla prolomena předřazená ochrana AACS – veškerý drahý hardware by nebyl k ničemu. A přesně to se stalo!

Zbytečné šifrování: Zní to zcela neuvěřitelně, neboť AACS používá silné 128bitové šifrování AES, které dodnes nikdo neprolomil. Toto šifrování aplikuje AACS na celou řadu klíčů, které mají obsah disku ochránit. Část těchto klíčů má v sobě přehrávač, ostatní najde na disku. Z obou těchto složek vypočítá tzv. Volume Unique Key (VUK), jímž pak filmový materiál dešifruje (viz rámeček na straně 62).

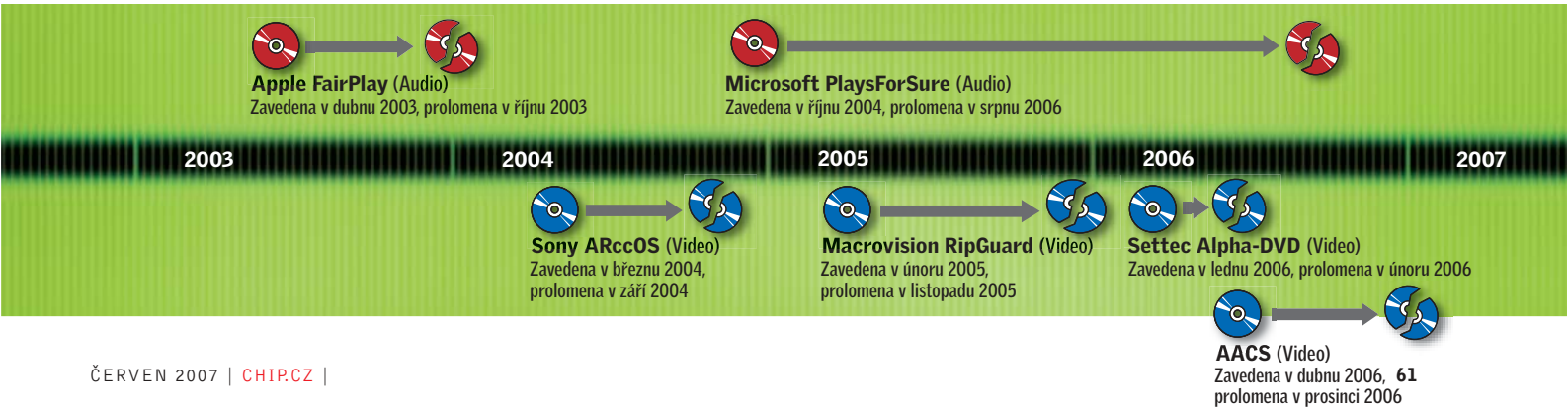
Vše, co na tom hackera zajímá, je tedy VUK. A jaké komplikované triky musí nasadit, aby klíč získal? Žádné – stačí mu založit kotouček do jednotky a přehrát jej v softwarovém přehrávači. Zároveň si otevře hexadecimální editor, například Winhex, načte do něj obraz paměti a v něm vyhledá VUK.

27. prosince 2006 o této slabině informoval jistý hacker pod pseudonymem „Muslix64“. A hned také připojil javovský program nazvaný BackupHDDVD, který umí ripovat HD-DVD. Nezveřejnil ovšem potřebné klíče VUK pro jednotlivé filmové tituly. Databanku, kterou nástroj potřebuje, si tedy musí uživatel naplnit sám. Proto také trvalo několik týdnů, než uživatelé zjistili, jaký znakový řetězec je třeba v paměti hledat a s kterým přehrávačem to jde. Mezitím se vyjasnilo, že se to daří s OEM verzemi softwarových přehrávačů WinDVD 8 a PowerDVD 6.5 a 6.6.

Muslix64 také brzy objevil, že tato mezera se vyskytuje i u Blu-ray přehrávačů, a promptně zhotovil nástroj BackupBluray. Kuriózní přitom je, že mu k tomu stačilo nahlédnout do specifikace BD a mít k dis- →



JAK OŠÁLIT APPLE: Všechny skladby zakoupené u iTunes osvobodí od jha DRM nástroj QTFairUse.



→ pozici výpis paměti, který mu kdosi poslal – šikovný hacker tedy celou věc zvládl, aniž by vůbec měl nějaký Blu-ray hardware.

Hackerské nástroje pro každého: Od té doby už ripování HD disků touto metodou přestalo být problémem i pro normální uživatele. Klíče VUK kolují na webu, ripovací software dostal grafickou ovládací plochu a jsou k dispozici i nástroje pro další zpracování filmových dat. A tak lze na výměnných burzách získat originální i překódované kopie HD filmů.

Na to vše musí výrobci zkompromitovaných softwarových přehrávačů nějak zareagovat. Cyberlink už tak učinil: v polovině února se objevil update pro PowerDVD Ultra, který má vyšpehování obsahu operační paměti znesnadnit – ještě dříve, než může editor obraz paměti uložit, přehrávač do ní zapíše nová data.

AACS LA, organizace odpovídající za protikopírovací ochranu, by samozřejmě mohla klíče OEM přehrávačů označit na nových discích za neplatné. Ta však vydala jen lakonické prohlášení, že samotné AACS je neporušené. Ukazuje se tak znovu, jak důležitá je korektní realizace zadaných úkolů.

Průlom č. 2: Lajdáctví průmyslu

Tomuto šlendriánu snad už bude konec. 5. února 2007 objevil hacker jménem „arnezami" další metodu, jak AACS přelstít – a už k ní není zapotřebí ani nečistě naprogramovaný prohlížeč. Stačí jen určitá disková jednotka a znalost funkce AACS.

Nechráněný tok dat: K odposlechu datového proudu mezi HD-DVD jednotkou od Microsoftu a počítačem použil arnezami nástroj „USB Sniffer", neboť USB spojení není zašifrované. Cíl je opět týž: zjistit hodnoty, z nichž se generuje VUK. Jen si tu blamáž představte: na jedné straně průmysloví velikáni jako Disney, Sony a Warner, kteří dlouho pracně vyvíjejí nenarušitelný řetěz protikopírovací ochrany, a na druhé straně Microsoft, jenž s klidem vrhne na trh mechaniku, která tento řetěz naruší hned na začátku.

NEODOLAL ANI HD-DVD: Nástroj BackupHDDVD ripuje filmy z HD-DVD na pevný disk po pouhém stisku tlačítka.

Předpověditelná identifikace média: To, na co arnezami narazil nejdříve, byl „Volume Identifier" neboli Volume ID (viz rámeček dole). A podle vlastních slov přitom nechtěl uvěřit svým očím. Podle specifikace AACS má mít totiž ID náhodně generovanou hodnotu. Realita je jiná: Volume ID na HD-DVD „King Kong" se skládá z data (18.09.2006) a času (08:41) →

Jak funguje AACS u Blu-ray a HD-DVD

Device Key Block: Každý přehrávač má svou sadu klíčů nazvaných Device Key. S těmito klíči prohledává Media Key Block na disku, aby zjistil, který Device Key potřebuje.

Media Key Block: Media Key Block sestává ze dvou částí. Jsou jimi „Identification Part" a „Key Data Part", přičemž každá položka v Identification Part je spojena s 16 bajty v Key Data Part.

1 Přehrávač nejprve prohledává položky v Identification Part. Najde-li položku, která odpovídá některému z jeho klíčů Device Key, dozví se tak zaprvé, který Device Key musí použít při dešifrování média, a zadruhé, kterých 16 bajtů z Key Data Part k tomu také musí extrahovat.

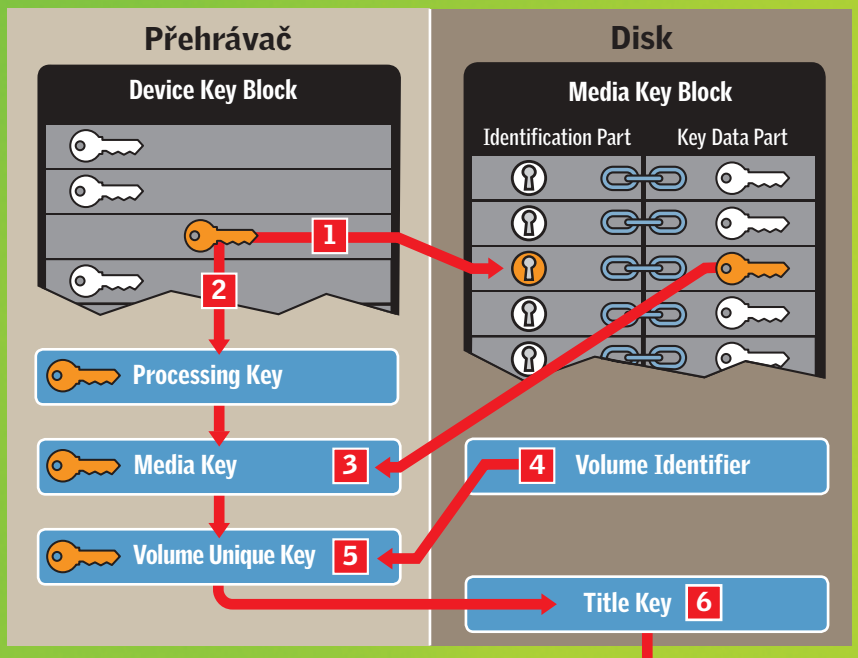
2 Pak přehrávač použije šifrování AES, aby pomocí Device Key vygeneroval Processing Key.

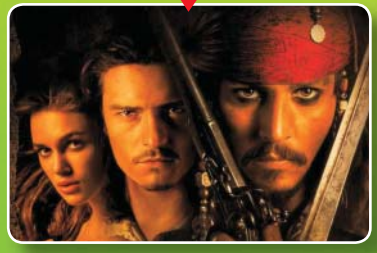
3 Nyní přehrávač vezme Processing Key a oněch 16 bajtů z Key Data Part. Na obě hodnoty aplikuje algoritmus AES a jako výsledek obdrží Media Key.

4 Dále přehrávač potřebuje Volume Identifier. Ten se nachází ve speciální části disku, která se nedá zkopírovat a vypálit na záznamové médium. To má u chráněného disku znemožnit kopírování „bit po bitu". Scheibe ausgeschlossen werden.

5 Na základě Media Key a Volume Identifier vygeneruje přehrávač Volume Unique Key (VUK). Ten má přístup do tabulky klíčů disku zvaných Title Key.

6 Title Key otevře zašifrovaný obsah disku – film se začne přehrávat.





→ výroby kotouče. Další uživatelé pak zjistili, že toto schéma platí i pro jiné filmové tituly. Volume ID se tedy dá předpovědět nebo alespoň po několika málo krocích odhalit. Mezitím byl dokonce zveřejněn „Private Host Key“ softwaru PowerDVD, jímž se prohlížeč dotazuje na Volume ID. Takto lze zjistit Volume ID každého DVD.

Jeden klíč pro všechny disky: Aby arnezami mohl VUK vypočítat, chyběl mu už jen „Processing Key“. Ten našel pomocí vlastnoručně napsaného programu v obrazu paměti zmanipulovaného přehrávače. Pikantní na tom je, že odhalený Processing Key platí pro každý kotouček na trhu, ať jde o Blu-ray, nebo o HD-DVD.

Stále stejný klíč – vypadá to jako lehkomyslnost, má to však svůj důvod: změna Processing Key by vlastně měla donutit AACS LA, aby zmanipulované přehrávače vyloučila. Nový Processing Key by mohla zvolit tak, aby ho klíče Device Key zmanipulovaného přehrávače už nemohly přečíst. AACS však všechny existující přehrávače považuje za nezkompromitované, a proto všechny disky používají tentýž Processing Key.

Pohroma u Sony

Audio CD a DVD Video byly koncipovány prakticky ještě za „analogových“ časů, a proti kopírování tudíž nejsou chráněny, nebo jen velmi špatně. Někteří výrobci se ve snaze zabránit tvorbě pirátských kopií uchýlili k poněkud drastickým metodám. Jejich cílem bylo, aby se tato média dala přehrávat ve stolních přehrávačích, ale nikoli zkopírovat v počítači.

CÉDÉČKA S ROOTKITEM: **Svou zhoubnou protikopírovací ochranou opatřil Sony celkem 52 CD titulů.**

■ **Havarovaná pécéčka:** Ve snaze zabezpečit své Audio CD si nejdrsněji počínal koncern Sony. Jeho protikopírovací ochrana XCP se totiž do počítače nainstaluje jako rootkit – s administrátorskými právy a bez vědomí uživatele. A jako by nestačil takovýto podraz, XCP zabraňuje nejen kopírování CD – ale i vypalování zvukových cédéček obecně. Protikopírovací ochrana působící jako filtrovací ovladač jednotek může dokonce způsobit havárii počítače.

■ **Drahá cédéčka:** Rootkitová aféra ukázala, že stará média by bylo možné zabezpečit jen za příliš vysokou cenu, kterou nejsou ochotni platit ani uživatelé, ani průmysl. Na tom protikopírovací ochrana tvrdě ztroskotala, a Sony nese výlohy: na základě soudního vypořádání zaplatí peněžitou pokutu ve výši 750 000 USD a každému postiženému zákazníkovi 175 USD – pro Sony tedy hodně drahá zkušenost.

Budoucnost: Všechno od začátku

Dnes už je jasné, že HD-DVD vyráběné od května dostávají nové klíče. Může to však někomu pomoci, když se stále ještě dají odposlechnout? Arnezami k tomuto účelu zveřejnil nástroj „aacskeys.exe“, který zaznamená všechny klíče HD disku.

Dá se AACS ještě zachránit? Stěží. Od února je na webu k dispozici Device Key pro WinDVD 8.0 a pro AnyDVD existuje verze, která ripuje disky Blu-ray i HD-DVD. Tímto nástrojem, který je šířen z karibského ostrova Antigua, může disky zkopírovat každý.

Markus Mandau ■