Bezpečnostní ochrany proti kopírování digitálních optických disků

Copy protection of optical discs

Jiří Růčka

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří RŮČKA**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní ochrany proti kopírování digitálních optických disků**

Zásady pro vypracování:

1. **Vypracujte literární rešerši popisující vývoj optických médií.**
2. **Prostudujte a popište ochrany používané na CD, DVD a Blu-Ray médiích.**
3. **Uveďte nejrozšířenější software sloužící k detekci a deaktivaci těchto ochran.**
4. **Uveďte možnosti výroby vlastního chráněného disku v domácím prostředí a otestujte jeho odolnost vůči deaktivačním nástrojům.**
5. **Uveďte právní možnosti kopírování optických disků v České Republice.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **HAVELKA, Jiří. Velká kniha vypalování CD a DVD. 2. aktualiz. vyd. Brno : CP Books, 2005. 470 s. ISBN 80-251-0629-2.**
2. **LOHNISKÝ, Jakub. 222 tipů a triků pro vypalování. 1. vyd. Praha : Computer Press, 2002. 94 s. ISBN 80-7226-634-9.**
3. **TAYLOR, Jim, et al. Blu-ray Disc Demystified. 1st edition. [United States of America] : McGraw-Hill, 2009. 432 s. ISBN 978-0-07-159092-1.**
4. **BRÜGMANN, Ulrich. Gecheckt -- Geheckt : Spiele kopieren. [United States of America] : Lulu Enterprises, 2007. 94 s. ISBN 978-3-00-022964-0.**
5. **CMAJDÁLKA, Lukáš. Metodika vyšetřování softwarového pirátství. [s.l.], 2008. 76 s. Vedoucí diplomové práce JUDr. Vladislav Štefka.**
6. **TAYLOR, Jim, JOHNSON, Mark R., CRAWFORD, Charles G. Velký průvodce DVD : Jedinečný zdroj všech dostupných informací o DVD na profesionální úrovni. 1. vyd. Praha : Grada Publishing, 2007. 552 s. ISBN 978-80-247-1721-0.**
7. **Deep in IT : Informace ze světa počítačů o hardware, software, Internetu atd. [online]. 2010 [cit. 2010-01-28]. Dostupný z WWW: .**
8. **Česká protipirátská unie [online]. [2010] [cit. 2010-01-28]. Dostupný z WWW: .**
9. **Autorský zákon [online]. 2009 [cit. 2010-01-28]. Dostupný z WWW: .**

Vedoucí bakalářské práce: **Ing. Petr Skočík**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá ochrannými technologiemi, které se používají k omezení či znemožnění kopírování chráněných dat z disku CD (Compact Disc), DVD (Digital Versatile Disc) a BD (Blu-ray Disc). Kromě popisu jednotlivých ochran proti kopírování je součástí práce i uvedení softwaru, který je frekventovaně používán a který funguje jako nástroj pro detekování nebo účinné obcházení ochrany, což vede k vytváření duplikátů. Aby nebyla zkoumána pouze továrně vyráběná média, opatřená ochrannou proti kopírování, je zmíněna možnost výroby vlastního chráněného disku a následné testování jeho odolnosti proti kopírování. Poslední uvedená oblast je věnována legislativě, platné na území České Republiky, která definuje možnosti vytváření kopií optických disků a v případě porušení daných zákonů i následné tresty.

Klíčová slova: kopírování, ochrana proti kopírování, optické disky, CD, DVD, Blu-Ray, vypalování, SecurDisc, ochrana dat, autorské právo, softwarové a audiovizuální pirátství

ABSTRACT

This project investigates various copy protection technologies used in the industry, which prevent or hinder illegal copying of protected data from CDs (Compact Discs), DVDs (Digital Versatile Discs) and BDs (Blu-ray Discs). Apart from describing the different copy protections, part of the project also discusses software which is used to detect or bypass these safeguards, which leads to the creation of duplicates. Although the project deals with commercial protected discs, it also looks into the creation of one's own protected discs and their subsequent testing against unauthorized duplication. The final section is dedicated to the legislature, effective within the Czech Republic, which defines options for legal duplication of optical discs, and the applicable consequences should the afore-mentioned laws be broken.

Keywords: copying, copy protection, optical discs, CD, DVD, Blu-Ray, burning, SecurDisc, data protection, copyright, software and audio-visual piracy

Děkuji svému vedoucímu Ing. Petrovi Skočíkovi za informace, rady a důležité připomínky, které vedly k úspěšnému dokončení této bakalářské práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Optické disky dnes patří k nejrozšířenějším médiím umožňující distribuci hudby, filmu, software, videoher nebo různých propagačních firemních materiálů, jako jsou například interaktivní katalogy prezentující produkty dané firmy. Důvodem, proč se optické disky dostaly na vrchol, je nejen jejich všestranné použití, ale také rozšířenost zařízení se schopností jejich čtení a relativně malé rozměry. Se zvětšujícím se objemem CD, DVD a Blu-Ray disků a stále dokonalejším hardwarovým a softwarovým vybavením, se zvyšuje i počítačová kriminalita, často nazývaná jako pirátství. Pod tímto označením si můžeme představit buď jednotlivce, nebo organizovanou skupinu, která se zabývá nezákonným kopírováním optických disků za účelem zisku.

Z důvodu zamezení výroby kopií se autoři a distributoři audiovizuálních děl a softwaru přiklánějí k nasazení tzv. ochran proti kopírování, které znesnadňují či znemožňují vytvoření funkční kopie. Problémem však je, že takové počínání vede k omezení poctivých uživatelů, kteří by si chtěli udělat jednu záložní kopii pro případ nechtěného zničení či ztráty originálního disku.

Zdokonalování a nasazování nových ochranných mechanismů je vždy reakcí na chování druhé strany, podílející se, ve snaze účinně obcházet ochrany proti kopírování, na vývoji softwarových aplikací pro jejich detekci a deaktivaci. Dostupnost těchto programů je díky Internetu maximálně rozšířená a riziko, že se chráněný disk stane předmětem napadení tak stoupá. Programy zmíněné v této bakalářské práci nejsou cílem jakékoliv propagace, ale jsou využity pouze pro vytvoření komplexního přehledu v dané problematice.

I. TEORETICKÁ ČÁST

1 STRUČNÝ VÝVOJ OPTICKÝCH MÉDIÍ

1.1 Kompaktní disk (CD)

Za první optický disk je považováno CD. Firmy Sony a Philips hledaly, po vinylových deskách a magnetofonových páskách, nové médium pro uložení hudby. V roce 1982 tak definovaly standard CD-DA (Compact Disc – Digital Audio). Specifikace pro audio CD byla uložena v červených deskách, proto je už od svého počátku nazýván tento standard jako Red Book neboli Červená kniha. [1]

Obr. 1. CD logo

V roce 1985 se objevil nový standard, vycházející z Červené knihy, pro ukládání počítačových dat s názvem CD-ROM. Jeho definice je uvedena ve žlutých deskách. Problémem tehdejší doby byly především CD-ROM mechaniky, které byly drahé a pomalé. Brzy se však přístupové doby a přenosové rychlosti díky novější technologii výrazně zlepšily. [1] Se zvýšením prodeje CD-ROM mechanik se postupně snižovala i jejich cena a tak i dostupnost široké veřejnosti. Variací vycházejících z Červené a Žluté knihy bylo samozřejmě v průběhu let mnoho, v této práci však budeme hovořit, vzhledem k ochraně obsahu, pouze o CD-DA a CD-ROM, proto je další členění zbytečné.

Obavy distributorů disků o rozšíření kopírování vzrostly s příchodem CD-R disku, CD-RW disku a vypalovacích mechanik. Možnosti ukládat své data na přenosné médium o kapacitě 650 MB představovalo značný luxus oproti dřívější 3,5" disketě, kde bylo možné zapsat 720 kB, 1,44 MB nebo nejvýše 2,88 MB. V současné době se s 650 MB (74 minutovými) médii už nesetkáme tak jako se 700 MB (80 minutovou) variantou. V souvislosti s vývojem stále dokonalejších vypalovacích mechanik si distributoři uvědomili, že nastává potřeba takovéto data chránit.

1.2 Digital Versatile Disc nebo Digital Video Disc (DVD)

Zanedlouho od průniku CD na trh se začalo mluvit už o jeho nástupci. Na trh se ale dostal až v roce 1996. O širokém rozšíření DVD se ale dá hovořit až na konci roku 1999. DVD

byla původně zkratka pro Digital Video Disc, tedy médium tvořené pro záznam videa. Vzhledem k tomu, že na DVD je možné ukládat prakticky jakékoliv data, bylo už ve specifikaci z roku 1995 nazváno Digital Versatile Disc, tedy digitální disk všestranného použití. Při tvorbě DVD-Video mluvily do specifikace i filmové studia, které měly rozsáhlé požadavky na ochranu obsahu, aby tak předešly obrovským ztrátám z nelegálního kopírování jejich filmů. [1]

Disky DVD by se podle obsahu daly rozdělit do následujících čtyř základních, nejvíce využívaných, skupin: DVD-Video, DVD-Audio, DVD-ROM a DVD-R / DVD-RW. DVD-Video je standardní DVD s filmem. Formát DVD-Audio přišel až čtyři roky po DVD-Video. DVD-Audio neobsahuje žádné video a jedná se pouze o vysoce kvalitní zvukový nosič, se kterým se dnešní člověk, až na malé výjimky, prakticky nesetká. Jednoduše se na trhu neujal a až na minimální počet vydavatelství ho neprodává nikdo. V hudbě vede stále audio CD. DVD-ROM, DVD-R / RW je prakticky obdobou CD-ROM, CD-R / RW. Varianta DVD-ROM je dnes, především pro vydavatelé produktů s vysokým objemem dat, nepostradatelná. Může se jednat například o encyklopedie, hry a další rozsáhlé softwarové produkty, které by si kvůli své kapacitě vyžadovaly větší počet kompaktních disků. A právě kapacita je další předností DVD nosiče. [1]

Obr. 2. DVD logo

Na rozdíl od kompaktních disků se DVD lepí ze dvou disků tenkých 0,6 mm, přičemž výsledné rozměry jsou shodné jako u CD. Jedním důvodem je jejich větší stabilita při čtení laserem ve vysokých otáčkách, dalším pak právě kapacita. Jedna strana může obsahovat až dvě vrstvy. Klasické jednovrstvé jednostranné DVD s kapacitou 4,7 GB má spodní stranu s jednou vrstvou. Na horní straně je přilepený pouze prázdný polykarbonát. [1]

Z hlediska kapacity, závislé na vrstvách a stranách, je možné DVD rozdělit do pěti skupin:

Označení	Kapacita v miliardách bajtů	Kapacita v giga bajtech	Strany a vrstvy
DVD-5	4,7	4,37	na jedné straně jedna vrstva
DVD-9	8,54	7,95	na jedné straně dvě vrstvy
DVD-10	9,4	8,75	dvě strany s jednou vrstvou
DVD-14	13,24	12,33	dvě strany, jedna a dvě vrstvy
DVD-18	17,8	15,91	dvě vrstvy na obou stranách

Tabulka 1. Kapacita DVD [1]

V případě DVD se ale rozlišují jednotky tzv. běžného a počítačového významu. Na klasickém DVD je uvedeno číslo 4,7 GB, po vložení do počítače má však už pouhých 4,37 GB. Zdůvodnit by se to dalo následovně. 1 GB = 1 000 000 000 B neboli 10^9, ale 1GB je taky v počítačovém světě 2^{30}, což je 1 073 741 824 B. Když nyní podělíme 1 073 741 824 číslem 1 000 000 000 a vynásobíme výsledek 4,37, vyjde nám opravdu přibližně 4,7 GB. [1]

1.3 Blu-ray disky (BD)

Kandidátů na třetí generaci optických disků bylo mnoho, hlavní boj se ale týkal disků HD-DVD a Blu-ray. Za HD-DVD se stavěla například Thoshiba, NEC nebo Sanyo, za Blu-ray pak Sony, Dell, Pioneer, Philips nebo LG. V roce 2008 bylo po pětiletém soupeření HD-DVD definitivně poraženo. Stalo se tak hlavně díky respektování Blu-ray předními filmovými vydavatelstvími a výrobci přehrávačů. Největší nevýhodou pro spotřebitele je, že Blu-ray není oproti HD-DVD zpětně nekompatibilní s mechanikami CD a DVD. Pro čtení i zápis se totiž používá modrofialový laser s menší vlnovou délkou. Filmová studia se pro Blu-ray rozhodla i z důvodu většího zabezpečení obsahu a větší kapacity oproti HD-DVD. [8]

Obr. 3. Blu-ray logo

Blu-ray disky byly vyvinuty za účelem sledování videa v širokoúhlém formátu 16:9 ve vysokém rozlišení, tedy maximálně 1920×1080 pixelů. Proto, aby bylo možné sledovat filmy ve vysokém rozlišení, je třeba rovněž větší kapacita BD než DVD. V současné době se vyskytují buď 25 GB, nebo 50 GB disky. Tato kapacita je ve skutečnosti, podobně jako u DVD, menší. Může být tedy zapsáno buď 23,3 GB na jednovrstvý disk, nebo 46,6 GB na dvouvrstvý disk.

I když byla technologie Blu-ray primárně navržená pro filmy, je na disky možné ukládat prakticky jakýkoliv datový obsah. Nezbývá, než čekat jakým dalším směrem se situace bude vyvíjet. Předpoklady jsou takové, že BD začne postupně vytlačovat DVD a jeho kapacita se bude zvyšovat až na hranici kolem 200 GB. Na paty BD však šlape holografický disk.

1.4 Pohled do budoucnosti

V budoucnosti bude poptávka po médiích s větší kapacitou stále růst, proto je jen otázkou času, kdy disky BD, které nejsou v dnešní době ještě příliš rozšířené, nahradí Holographic Versatile Disc (HVD). O holografických discích se mluví už dlouhou dobu, byly dokonce už několikrát představeny od výrobců jako Sony nebo InPhase Technologies. S holografickým diskem se počítá jako médiem určeným pro záznam 3D filmu. [18] Nejdříve se mluvilo o disku s kapacitou 250 GB, později 500 GB, dnes je už jisté, že jejich potenciál je v řádech jednotek až desítek TB. Dle vyjádření americké společnosti GE (General Electric), která stojí rovněž za vývojem holografického disku, by měly být jejich disky dobře čitelné s menší úpravou dnešních Blu-ray přehrávačů. [17] HVD disponují rovněž větší spolehlivosti z hlediska trvanlivosti dat a vyšší rychlosti čtení.

Obr. 4. HDV logo

Odhadování jakéhokoliv vývoje je vždy složitá situace. Jedna věc je však jasná, přenosové rychlosti, kapacita a nároky na spolehlivost se budou nadále zvyšovat.

2 IMPLEMENTACE OCHRANY NA LISOVANÝ DISK

2.1 Mastering

V oblasti masteringu začíná výroba lisovaného disku. Tady se provádí zavádění dat, které dodal zákazník, do počítače. Stejně tak se už tady provádí opatření disku ochranou proti kopírování. Data můžou být dodána na CD, DVD, jiném médiu nebo si je operátor masteringu stáhne z Internetu. Po zadání dat do počítače dochází ke spuštění procesu, při kterém se data z počítače převádějí na svit laseru, který v závislosti na zapisovaných datech osvítí pouze některá místa skleněné kruhové desky. Ještě před zápisem dat se nanese na tuto desku tenká fotocitlivá vrstva. Po osvícení je deska, podobně jako film, „vyvolána“. Na místech, kde dopadl svit laseru, zůstanou pouze prohlubně. Kdyby existovalo zařízení k přehrávání takového polotovaru, byly by datové informace čitelné, jeho kopie by však byla obrácená. Pro vytvoření kopie je proto třeba vytvořit nejdříve negativ desky – matrici. [5]

2.2 Vytvoření matrice

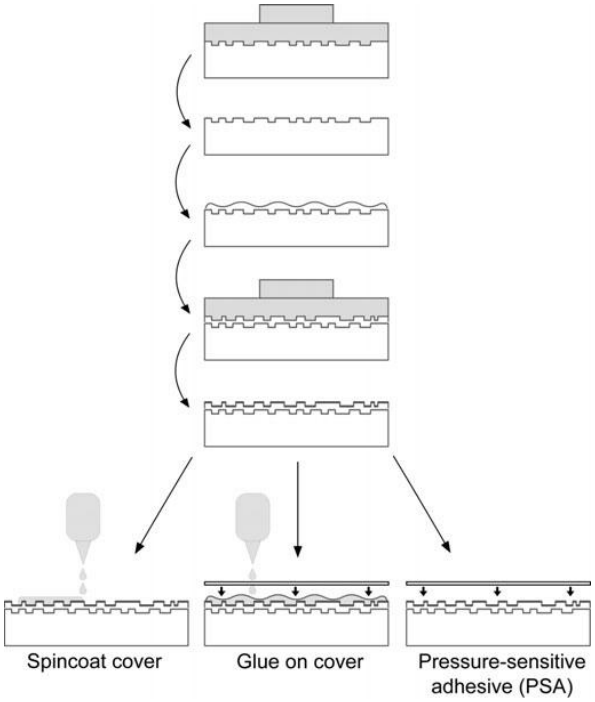
Na skleněnou desku s prohlubněmi je galvanicky nebo vakuově nanesená tenká vrstva zinku nebo jiné slitiny. Následuje pokovení další silnější vrstvou – stříbrem. Taková vrstvička se odloupne od, zinkem pokovené, skleněné desky a vznikne potřebný negativ (tzv. otec). Proces tímto není ještě u konce, i když by to tak mohlo vypadat. Náklady na výrobu „otce“ jsou vysoké, proto se proces výroby matrice rozšiřuje o výrobu dalších pozitivů (tzv. matek). Z „matek“ se pak vyrobí už finální negativy, které jsou používány pro lisování CD a DVD. Takovému finálnímu negativu se říká matrice, raznice nebo dokonce i „syn“. [5]

2.3 Lisování disku a další úpravy

Základní surovinou pro výrobu je polykarbonát maximální optické kvality. Polykarbonát se dopraví do lisu, roztaví se a vstříkne se do formy, kde už je připevněná vyrobená matrice. Pod vysokým tlakem +/- 100 tun se vyrazí informace z matrice na polykarbonát. Tak vznikne plastový kotouč, na kterém jsou data. Aby mohl laser v přehrávacích mechanikách data snadno číst, nanáší se na povrch kotouče reflexní vrstva z hliníku. Ta je však náchylná na oxidaci. Řešením je použití ochranného krycího laku a potisku. [5]

V případě DVD a Blu-ray je postup skoro stejný, rozdíl je pouze v tom, že se u těchto médií používají dvě vrstvy polykarbonátu spojené tenkou vrstvičkou lepidla. Existují dva způsoby výroby. Prvním je otisknutí matrice první vrstvy do jednoho substrátu a následné přidání napůl odrazivého filmu. Poté se vezme druhý substrát a vzhůru nohama se do něj otiskne matrice druhé vrstvy, přidá se na ní plně odrazivý film, otočí se a přilepí se k prvnímu substrátu. [8]

Druhá frekventovanější metoda, viditelná na obrázku, je použití prázdného substrátu a substrátu, v němž jsou vyraženy obě vrstvy. Do substrátu se vyrazí matricí první vrstva, na ní se přidá napůl odrazivý film a průhledný materiál v podobě ultrafialové pryskyřice. Do ní se otiskne druhá vrstva, přidá se plně odrazivý film a pak už se jenom přilepí druhý 0,6 mm prázdný polykarbonátový substrát. [8]

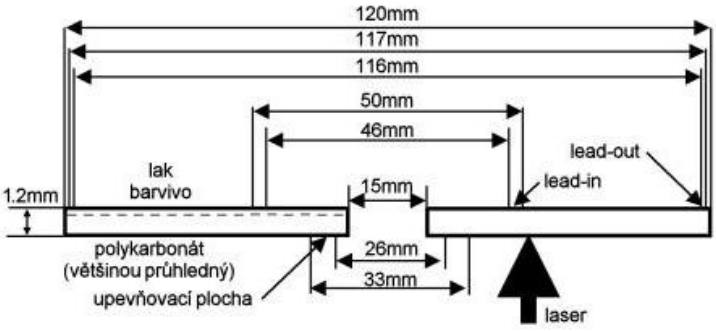


Obr. 5. Lisování dvouvrstvého Blu-ray disku

3 ZÁKLADNÍ TECHNICKÉ PARAMETRY OPTICKÝCH DISKŮ

3.1 Rozměry

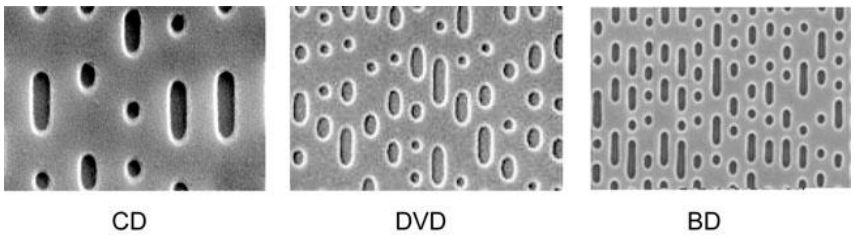
Při zkoumání všech standardních optických disků zjistíme mnoho společných znaků, které se týkají jejich rozměrů a hlavních oblastí. Standardizovaným rozměrem je kotouč s průměrem 120 mm a tloušťkou 1,2 mm, v jehož středu je kruhový otvor o průměru 15 mm. Data jsou zapisována v oblasti od 46 mm do 117 mm. [5]



Obr. 6. Rozměry a hlavní oblasti CD [2]

3.2 Struktura uložených dat a jejich čtení

Data jsou na disku zapsána ve spirále, která je jak čtena, tak zapisována od středu k okraji. Na CD, DVD a BD jsou data prezentována pomocí prohlubní (pitů) a výstupků (landů) bez ohledu na to, zda byla vypálena nebo vylisována. Čtení těchto dvou hodnot probíhá pomocí laserového paprsku. Podle velikosti odraženého světla fotodioda určí, zda se jedná o oblast pit nebo land. Pokud se jedná o pit, tak dochází k rozostření paprsku v prohlubni a fotocitlivá součástka zaznamená hodnotu „tma“. V případě landu je paprsek odražen od výstupku a putuje přes optický hranol k fotocitlivému členu, kterému ohlásí hodnotu „světlo“. Tyto informace se přeloží do podoby jedniček a nul. Jedničky jsou na hranách mezi pitem a landem, zbytek jsou nuly. [9]



Obr. 7. Zvětšená struktura CD, DVD a Blu-ray [1]

Z výše uvedeného obrázku je patrné, že data uložená na DVD mají, na úkor zvýšení kapacity, zhuštěnou strukturu. Při srovnání CD a Blu-ray je rozdíl už obrovský.

Druh média	Rozteč drážek [μm]	Vlnová délka laseru [nm]	Barva laseru
CD	1,6	780	červená
DVD	0,74	635 až 650	červená
Blu-ray	0,32	405	modro-fialová

Tabulka 2. Čtení dat na CD, DVD a Blu-ray

U dvouvrstvého DVD nebo Blu-ray laser postupuje při čtení vzdálenější vrstvy tak, že zvýší svůj výkon a první vrstvu ignoruje. [9]

3.3 Pojem sektor, TOC a session

Při používání ochran proti kopírování se na disk často implementují společně s daty taky slabé nebo vadné sektory. Sektor je základní datovou jednotkou na všech optických discích, přičemž velikost sektorů a informace uvnitř sektoru se na jednotlivých typech nosičů liší. Kromě samotných dat můžou obsahovat sektory taky bajty pro korekci chyb. V případě DVD-Video se v sektoru taky vyskytuje i jeho základní ochrana CSS. [5]

Některé ochrany kopírování u CD, jako třeba Cactus Data Shield zmíněná dále, využívá chybných údajů v TOC tabulce, proto by bylo dobré vědět, co taková tabulka obsahuje. Jedná se o informativní údaje pro mechaniku. TOC definuje začátek každé stopy, jejich délku i počet všech stop. Kterákoliv session na CD má svoji TOC. Hlavní TOC obsahuje údaje o všech session. [3]

U všech optických disků existuje možnost nahrát data najednou nebo s určitou časovou prodlevou. Data nahrána v jednom souvislém celku tvoří jednu session. Pojem multisession se používá pro optické disky s více session. Hudební CD je tvořeno pouze jednou session. Může mít prakticky ale i dvě, kdy druhá je použita například pro bonusové materiály jako videa nebo fotografie, takové médium pak nese název CD-Extra. Problém s přehráváním nenastane, protože stolní audio přehrávače mají schopnost číst pouze první sekci. [3]

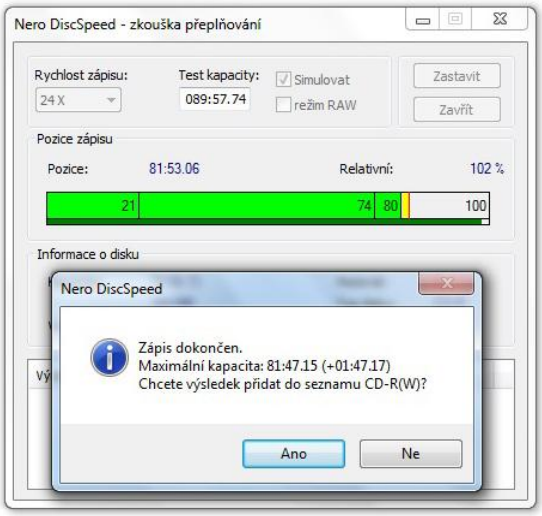
4 HISTORICKÝ VÝVOJ OCHRAN PROTI KOPÍROVÁNÍ

4.1 Přeplňování disku

Ochran proti kopírování je celá řada, některé můžeme jednoduše vypnout, jiné komplikovaně a samozřejmě existuje i několik dosud neprolomených. Ačkoliv se často jedná relativně o silné opatření, tak se dříve nebo později najdou vynalézaví lidé, kteří přijdou na ten správný způsob, jak takovou ochranu deaktivovat. [4]

Jednoduchou ochranou proti kopírování bylo lehké přeplnění standardního 650 MB kompaktního disku, tzv. „overburn“. [22] Dnes tato primitivní technika nemá takový význam hlavně díky 700 MB CD. Stejně tak můžeme přeplnit i 700 MB variantu a pravděpodobnost, že se najde médium se stejnou velikostí místa navíc pro přeplnění, je velká. Technika jde dopředu a na to musí reagovat i výrobci digitálních optických disků, tedy výrobci ochranných technologií.

Dnes prakticky každá vypalovací mechanika zvládá výrobu takto chráněného disku, je nezbytné ale vědět, že přeplňování není zas tak bezpečné. Při takové operaci se může nenávratně zničit vypalovací mechanika. Protože laser najede při zapisování lead-out o něco málo blíže okraji disku. Takto se ale může stát i samotné CD na některých starších mechanikách nečitelné. U DVD se při standardním pálení nedoporučuje ani kompletní vyplnění 4,5 GB. [5]



Obr. 8. Test maximální kapacity CD

Čím jsou totiž zapsaná data blíž okraji DVD, tím jsou, vlivem času a podmínek skladování, hůře čitelná. Informace o tom, jaká je skutečná kapacita CD a DVD lze zjistit například nástrojem DiscSpeed z balíku vypalovacího softwaru Nero. [5] Z obrázku výše je patrné, že kapacita testovaného 703 MB CD lze, s možným rizikem, rozšířit až na 717 MB.

4.2 Vadný obsah TOC

Dalším mezníkem v datové bezpečnosti na CD bylo pozměnění obsahu TOC. Jak už bylo zmíněno výše, jedná se o uvedení začátku a konce každé stopy a její velikosti. Takže se klidně stávalo, že tato tabulka ohlásila, na tehdejší dobu, utopickou myšlenku, že se na CD vyskytuje např. 2 GB dat. Většina tehdejších CD rekordérů udělání kopie takového disku samozřejmě odmítla. Tohle opatření bylo časem taky napadeno, proto se začalo pracovat na vývoji technologie, kterou by vypalovací mechanika nebyla schopná zapsat – vadné sektory. [4]

4.3 Vadné neboli oslabené sektory

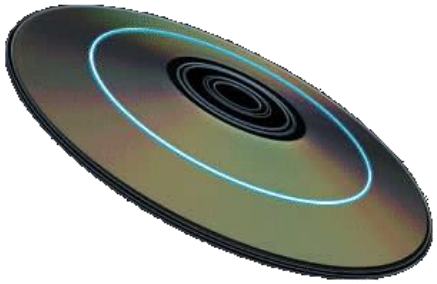
Vadné sektory byly začleněny přímo mezi data na disku. Princip je takový, že mechanika se snaží číst pouze data, která neobsahují chyby, pokud se vyskytne chyba, tak dostaneme upozornění v podobě hlášky na obrazovce. Oblasti s vadnými sektory se vyskytují většinou na začátku disku než na jeho konci. Nejedná se však pouze o chyby vložené na disk při masteringu, ale taky další softwarové řešení, které je v další kapitole zmíněno u každé ochrany.

Dnešní vypalovací mechaniky mají, v součinnosti se speciálním softwarem, možnost pracovat i s těmito vadnými sektory. Vývoj CD a DVD rekordéru je nezastavitelný a právě tady vzniká boj mezi výrobci lisovaných disků a druhou stranou, která je zastoupena výrobci dokonalejších mechanik a softwaru k vyřazení těchto oslabených míst. [4]

5 OCHRANY PROTI KOPÍROVÁNÍ DATOVÝCH DISKŮ

5.1 Ring Protech

Jak již název napovídá, tak ochranu „Ring Protech“ snadno poznáme podle viditelné kružnice, která se nachází zhruba uprostřed disku. S touto ochranou přišla na trh japonská firma Ed-contrive. Pouze pohledem se tak můžeme ujistit, zda se jedná o originální CD nebo jeho pirátskou kopii. O této ochraně, která byla představena v druhé polovině roku 2001, bylo prohlášeno, že by měla naprosto zamezit pirátství. Nestalo se tak. [10]



Obr. 9. Prstenec u Ring Protech

Ochrana spočívá v těžko kopírovatelných (ideálně nekopírovatelných) souborech, uložených v asi 1mm široké kružnici uprostřed disku. Při spouštění aplikace na disku jsou soubory v tomto prstenci kontrolovány. Pokud nejsou nalezeny, aplikace se nespustí. [10]

5.2 Alcatraz

Technologii Alcatraz začala používat v létě roku 2000 rakouská společnost KDG. Alcatraz využívá technologie tzv. vodoznaku, kdy je prováděná úprava chráněné aplikace už během tvoření skleněné matrice použité k lisování. [2]

Alcatraz je technologie založená na vodoznaku a spustitelném ochranném systému. Alcatraz poskytuje čtyři úrovně ochrany.

- Úroveň 1 je nejnižší úroveň ochranného systému, která znemožňuje kopii na 74 minutový disk CD-R.
- Úroveň 2 poskytuje rozsáhlejší ochranu v podobě zamezení čtení a kopírování dat za pomocí standardních softwarových nástrojů, které slouží ke kopírování CD.

- Úroveň 3a je směrována přímo proti profesionálním pirátům. Pirátská kopie takového disku je prakticky nepoužitelná. Tato bezpečnostní ochrana umožňuje nezávislé testování a rozpoznávání originálu.
- Úroveň 3b, jako nejostřejší verze ochrany proti kopírování, přichází ve formě „ochranné vrstvy“, kterou je aplikace na disku opatřena již při samotném masteringu. Tato ochrana částečně či úplně zabraňuje instalaci aplikace, jestliže je zjištěno, že se jedná o ilegální kopii. Podle vyjádření KDG je schopná zobrazit nejen výstražnou zprávu, ale i způsobit kolizi operačního systému nebo dokonce naformátovat pevný disk počítače. [11]

Obr. 10. Alcatraz

5.3 SafeDisc

SafeDisc je CD / DVD ochrana proti kopírování pro Windows aplikace. Ochrana je od roku 2000 vyvíjena společností Macrovision. SafeDisc přiřazuje při výrobě unikátní digitální podpis každému optickému médiu. Při každém spuštění programu provádí SafeDisc kontrolu takového digitálního podpisu. Ověření trvá běžně 10 – 20 sekund, po verifikaci se spustí program naprosto běžným způsobem. Podpis SafeDisc je navržen tak, aby nebylo jednoduché ho zkopírovat na jiný disk. Většina běžných programů nepotřebuje po nainstalování na pevný disk počítače zdrojový instalační disk v CD-ROM jednotce, programy chráněné SafeDisc však běží pouze s přítomností zdrojového média v mechanice. [2] Podobně jako u ochrany Alcatraz existují i u SafeDisc čtyři úrovně zabezpečení.

SafeDisc 1 – takto chráněný originální disk obsahuje velké množství nečitelných sektorů, tvořící celkem přibližně 20MB. Chyby se vyskytují nejčastěji mezi 800 a 10 000 sektorem. SafeDisc první verze by měl obsahovat soubory 00000001.TMP, CLCD16.DLL, CLCD32.DLL, CLOKSPL.EXE, DPLAYERX.DLL, <HRA>.EXE a <HRA>.ICD [17]

Název <HRA> nahrazuje skutečný název hry nebo programu. EXE soubor je pouze zavaděč, který dešifruje a načte chráněné soubory, který je potřebný ke spuštění hry. Tyto soubory jsou zašifrované v souboru s koncovkou ICD. Vyrobení fungující kopie bylo jak pro domácí uživatelé, tak pro profesionální duplikátory u první verze velice jednoduché, stačilo si dešifrovat soubor ICD a převést si je na EXE. [2] Tento problém byl napraven v září roku 2000 s vydáním druhé, o něco úspěšnější, verze.

Obr. 11. SafeDisc

SafeDisc 2 – stejně jako první verze, pracuje s velkým množstvím vadných (nečitelných) sektorů, mimo to se objevují i oslabené sektory, způsobující některým vypalovačkám značné synchronizační problémy. Druhou verzi lze rozpoznat podle souborů 00000001.TMP a 00000002.TMP. [2]

Zaváděcí soubor <HRA>.EXE je integrován do hlavního spustitelného souboru, tím je eliminováno riziko jeho dešifrování. Takto chráněná CD jsou téměř 100% funkční na všech typech mechanik. Taky díky tomu označila firma Philips SafeDisc 2 jako odpovídající standardům Yellow Book. Třetí verze se dostala na CD v roce 2003 a přinesla s sebou další vylepšení. [2]

SafeDisc 3 – disponuje možností používat virtuální mechaniku. Virtuální mechanika je disková jednotka, která se v počítači fyzicky nevyskytuje, ale je emulována pomocí programů jako Alcohol 120% nebo Daemon Tools a umožňuje spuštění image souborů, tedy kompletního obrazu skutečného disku. Nutností u třetí verze zůstává ověření digitálního podpisu ze zdrojového originálního CD / DVD. Velikost digitálního podpisu se pohybuje od 3 do 20MB v závislosti na kvalitě šifrování. [2]

Obr. 12. SafeDisc Advanced

SafeDisc 4 – nejnovější verze je používána od roku 2006. V dnešní době nese označení Advanced. SafeDisc Advanced využívá většina předních vydavatelství her. Novinkou je

použití technologie Asymmetric Code Blending, která pirátům ztěžuje odstranění bezpečnostních komponentů bez vlivu na hru. Taková nepovedená pirátská verze může způsobit, že hra nepůjde ani dohrát do konce. Důvodem může být třeba nefunkční auto, kterým je třeba dojet na místo určení nebo neustálý chod hry v určité smyčce dokola. [12]

5.4 StarForce

StarForce by se dala označit jako nejkontroverznější a nejdiskutovanější ochrana, která je dokonce schopná zničit i hardware počítače. Výrobce ochrany ale něco takového pochopitelně odmítá. Ruská společnost StarForce Technologies se tak snaží, už od roku 1998, omezovat počítačové pirátství. Původně byla cílem pouze implementace ochrany v zemích východní Evropy, postupně ale byla StarForce patentována v celé Evropě i Americe.

Obr. 13. Ochrana StarForce

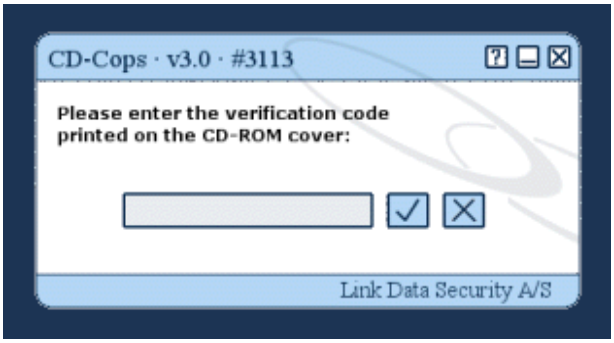
StarForce využívá šifrování samotných dat, využívá systémové ovladače a kontroluje fyzickou struktury média. Jak už to většinou u těchto ochran bývá, nevedou přímo k ochraně, ale především k plození další počítačové kriminality a potížím s funkčností. Některé verze StarForce například kontrolují pravost média změřením úhlu mezi prvním a posledním sektorem na disku. Vzhledem k tomu, že jde o přesný úhel, pouhé poškrábání nebo drobná odchylka výroby může vést k tomu, že se dostaneme do stejné situace jako vlastníci ilegální kopie. [4]

V současné době je StarForce nabízena ve třech verzích. Nejjednodušší je verze Basic, která do počítače neinstaluje žádné ovladače. Skrytý ovladač instaluje do systému až varianta Pro. Nejsilnější varianta Elite je prakticky nepoužívaná, protože jsou s ní spojeny i největší komplikace a to jak na straně profesionálních pirátů, tak na straně běžných uživatelů. [19]

5.5 CD-Cops a DVD-Cops

Dánská společnost Link Data Security, zabývající se ochranou dat skoro dvacet let, přišla v roce 2001 s CD-Cops. Za tuto dlouhou dobu nejen zdokonalovala své ochrany, ale zároveň si budovala pevné místo na trhu. Dnes patří Link Data Security mezi přední vývojáře a poskytovatelé těchto služeb. Mimo jiné se firma specializuje i na zabezpečování dat na dalších přenosných médiích a poradenstvím v zabezpečení dat. [13]

Ochrana CD-Cops pracuje na principu ověřování doby čtení určitého fyzického úseku na disku. Pokud ověřovací systém zjistí, že se doba čtení liší, program nebudeme moci nainstalovat. Abychom mohli spustit vlastní měření, musíme nejprve, po vložení CD do mechaniky, zadat verifikační kód uvedený na CD nebo jeho obalu. Kromě okna, na obrázku níže, lze poznat takto chráněné médium i podle souboru CDCOPS.DLL a souborů s příponou .GZ_ a .W_X. Za zmínku stojí i striktní dodržování standardů Yellow Book. [2]



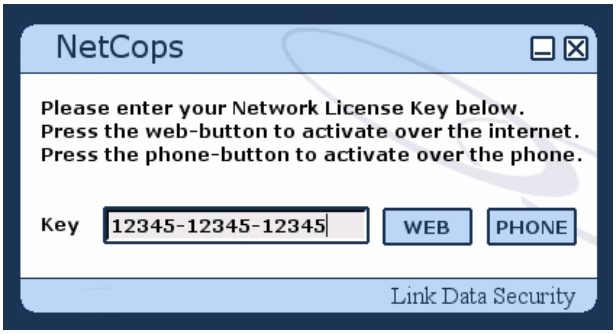
Obr. 14. Zadání verifikačního čísla u CD-Cops

Stává se skoro pravidlem, že výrobci poskytují více úrovní u jednotlivých bezpečnostních ochran. Link Data Security nabízí tyto verze:

Standardní verze (Standard): Verifikační klíč je kontrolován při každém zahájení programu.

- Rozšířená verze (Enhanced version): Je ideální pro dokonalé zabezpečení, existuje možnost provádění dalších verifikačních kontrol (Key-CD check) na různých místech CD.
- Instalační verze (Machine Install version): Verifikační klíč (Key-CD) se zadává pouze při instalaci, při dalším spuštění není klíč vyžadován. Výhodou je možnost nainstalování aplikací na několika počítačích ze stejného CD.

- Verze s pevnou dobou ukončení platnosti (Hard expiry version): Kontrola probíhá při každém spuštění programu. Spuštění programu je možné pouze po určité období, datum je absolutní (nejedná se např. o 30 denní verzi, ale je uveden přesný den konce platnosti např. 21. 12. 2012), může být použitá pro demo verze programů.
- Verze s pravidelným vkládáním klíče (Regular key-CD insertion): Kontrola probíhá pouze jednou za čas (běžně 2 – 4 týdny, interval může být vybrán). Obsahuje varování několik dní před vypršení platnosti.
- Zabezpečení v rámci sítě (Network security): Verze pro větší organizace i školy. Originální CD je ověřeno, soubory jsou zkopírovány na server a správce sítě musí zadat licenční klíč. Každý uživatel v rámci sítě, který spustí aplikaci je automaticky přihlášen a nemusí vyplňovat klíč. Počet současně pracujících uživatelů nesmí překročit počet, který povoluje licence, pokud bude počet překročen, uživateli se zobrazí zpráva o možnosti dokoupení licence a aplikace se nespustí. [13]



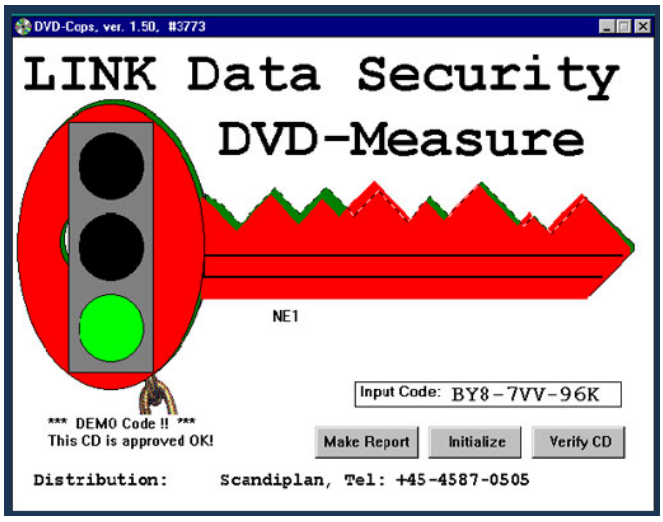
Obr. 15. Zadání verifikačního čísla pro PC síť

Společnost Link Data Security nabízí ochranu i u běžných CD-R disků. Tato ochrana je vhodná hlavně pro malé produkce a nese název CDR-Cops. Hlavní výhodou je snížení finančních nákladů potřebných na výrobu matrice pro lisování CD. Bezpečnost je na stejně vysoké úrovní jako u CD-Cops. Produkce chráněného CD-R je prováděna přes vlastní vypalovací mechaniku a pomocný softwarový modul, který je součástí balíčku CDR-Cops. Při takovémto postupu tvorby chráněného CD je možno použít prakticky jakýkoliv prázdný disk CD-R a klasickou vypalovací mechaniku a software. [13]

Postup výroby je následující: Nejprve se spustí program CDR-Cops a provede se potřebné nastavení. Poté uživatel běžným způsobem spustí vypalování, které by mělo trvat stejnou dobu jako u pálení nechráněných CD. Rozdíl je zde v nutnosti připojení na internet během

vypalování, to může vést k drobnému prodloužení vypalovacího procesu. Další komunikace s internetem slouží pro ověření CD, není tak nutné zadávat verifikační kód, který u lisovaných CD najdeme na obalu. [13]

Od stejné společnosti pochází i DVD-Cops. Jedná se o první protipirátskou ochranu, která byla u média typu DVD-ROM použita. Je založena na stejném principu jako CD-Cops. Ochrana byla dokončena v polovině roku 1998, první nosič se však dostal na trh až v říjnu. [13] Vzhledem k nárůstu cen originálních DVD, poklesu cen vypalovaček a DVD-R/RW médií rychle narostla popularita této bezpečnostní technologie.



Obr. 16. Zadání verifikačního čísla u DVD-Cops

Samozřejmostí je i šest verzí této ochrany, podobně jako u CD-Cops, a stejně tak domácí výroba chráněného disku s názvem DVDR-Cops. Postup výroby je naprosto shodný jako u CD varianty. [13]

5.6 CopyLok

CopyLok vznikla v roce 2001 spoluprácí společností Pan Technology Limited a Toolex International N.V.. Vzhledem k tomu, že se tato ochrana používala poměrně málo, ani informací o ní není mnoho. Ochrana pracuje na technologii vodoznaku na CD, její identifikace je možná podle jinak zabarveného prstence na disku, který se běžně nachází mezi 2000 a 10000 sektorem. CopyLok je hodně podobný technologii SafeDisc. Podíváme-li se na EXE soubor, zjistíme, že obsahuje soubory s příponou ICD (konkrétně icd1, icd2,…), které byly použity u SafeDisc. Na CD se nenachází jednoznačné identifikační soubory, jako například 00000001.tmp u SafeDisc, ani další adresáře. Veškeré ochranné

prostředky jsou zabudované v tomto EXE souboru. V dnešní době se tato ochrana považuje za prolomenou a již se nevyužívá. [2]

5.7 DiscGuard

V roce 2000, kdy firma TTR Technologies poprvé použila tuto ochranu, patřila mezi nejúčinnějším proti pirátství. Neměla ale dlouhé trvání, protože byla brzy nahrazena účinnější ochranou konkurence SafeDisc 2. Dnes považujeme tuto ochranu za zastaralou a nepoužívanou. Po nainstalování programu do počítače, lze ochranu DiscGuard jednoduše identifikovat podle souborů IOSLINK.VXD a IOSLINK.SYS v adresáři, do kterého byl program nainstalován. Skleněná matrice, která se používá při výrobě, přidává na CD kromě dat i „digitální podpis“. Tento podpis je běžným způsobem nekopírovatelný. V případě použití originálního CD dojde k přečtení takového podpisu, jeho verifikaci a spuštění programu. [2]

5.8 LaserLock

LaserLock je velmi populární a hojně používaná ochrana veškerého obsahu CD-ROM i DVD-ROM nosičů. Pochází z dílny společnosti MLS LaserLock International založené v roce 1989 v řecké Soluni. MLS LaserLock International je první společností, která vyvinula kompletní softwarový systém ochrany proti kopírování, zvláště pro CD-ROM nosiče. Díky tomu vyhrála i prestižní cenu „European IT Grand Prize Award“. Systém ochrany LaserLock je patentován po celém světě a jeho úspěšnost stále roste. Společnost se pyšní jednou z nejlépe vybavených CD-ROM a DVD-ROM laboratořích v Evropě. Mimo ochranu optických disků se společnost zabývá také ochranou dat na paměťových kartách a USB klíčenkách. [14]

Obr. 17. LaserLock

CD, které je opatřené LaserLock, obsahuje skrytý adresář LASERLOK, uvnitř kterého najdeme soubor LASERLOK.IN. Ano LASERLOK, nikoli LASERLOCK, ochrana je totiž kompatibilní se systémem DOS, který umožňoval pouze osm znaků. Předposlední znak je

tudíž vypuštěn. Další rozpoznání je možné vizuálně, pohledem na datovou oblast CD. K vidění je několik kružnic, u starší verze pak jen jedna. Kružnice obsahuji nečitelné části a vyskytují se od sektoru 2 100 do 6 200. [2] Na každém CD-ROM, CD-R nebo DVD je při výrobě vsazen unikátní fyzický podpis, který je odlišný pro každou aplikaci. Když se aplikace spustí, kontroluje se umístění podpisu a jeho velikost. LaserLock pro CD-ROM a CD-R zabírá 20MB na disku, pro DVD-ROM 40MB. Na žádost zákazníka může být použita i menší velikost, ale na úkor bezpečnosti. [14]

Jak už bylo naznačeno, tak je možno chránit touto technologií i obsah na CD-R. S podobnou technologií se můžeme setkat u CD-Cops / DVD-Cops, ale s tím rozdílem, že LaserLock dosud neposkytuje domácí záznam na DVD-R. [14]

5.9 Shrnutí kapitoly

Z předchozích několik stránek vyplývá, že veškeré zmíněné technologie pracují prakticky na stejném principu. Vodoznak, digitální podpis nebo fyzický podpis je prakticky totéž, tedy vložení na disk společně s daty chybné sektory a následná kontrola jejich přítomnosti. Jakousi výjimku tvoří CD Cops a DVD Cops, který kontroluje dobu čtení určitého fyzického úseku na disku. Na vývoji ochran proti kopírování datových disků se podílí samozřejmě více společností. Jejich vyjmenovávání by bylo ale naprosto zbytečné, úkolem práce je totiž podat informace o nejpoužívanějších ochranách.

Nasazení ochran u disků se softwarem je v porovnání s filmovými a hudebními nosiči největší, proto je tato kapitola obsahově nejrozsáhlejší. Ochrany dat na DVD-Video a Blu-ray netvoří tak obsáhlou kapitolu s komerčními ochranami taky proto, že už při samotné koncepci jejich standardů byl kladen velký důraz právě na ochranu jejich obsahu.

6 OCHRANY PROTI KOPÍROVÁNÍ HUDEBNÍCH CD

6.1 Cactus Data Shield

Je forma ochrany hudebních CD, která se vyvíjela od roku 1999 izraelskou společností Midbar Tech. Nynějším vlastníkem je společnost Rovi. Tato ochrana je používána především vydavatelstvími EMI a BMG. CDS mírně mění informace uložené na CD. Ochranu lze jednoduše identifikovat při vložení CD do CD-ROM mechaniky, podle 99 nesmyslných a nefunkčních datových stop. Ve stolních audio přehrávačích by se něco takového nemělo stát a disk by se měl chovat jako kterýkoliv jiný. Upozornění, že CD není možno přehrát v CD-ROM mechanikách lze nalézt zpravidla jak na bookletu, tak i na samotném disku. [2] CDS existuje ve třech verzích.

Obr. 18. CDS logo a označení třech různých verzí

Alba obsahující CDS-100 je možné přehrávat pouze na klasických CD přehrávačích, na počítačích by se neměly vůbec chovat jako audio kompaktní disk. Tahle verze je nejlepší pro maximální ochranu proti pirátskému zneužití. [2]

CDS-200 navíc umožňuje přehrání jak na počítači, tak na stolním přehrávači. [2]

Třetí verzi CDS-300 přehrajeme na obou zařízeních, navíc máme možnost hudbu z kompaktního disku zkopírovat, pomocí správy digitálních práv (DRM, Digital Rights Management), na pevný disk počítače. Skladby na CD přehrajete ve svém počítači dvěma způsoby. Prvním způsobem je přehrávání s vloženým CD pomocí programu Windows Media Player (WMP). Druhý způsob umožňuje zkopírovat soubory pomocí WMP na pevný disk počítače a následně přehrávat skladby v tomto programu bez zdrojového disku. Výrobce uvádí, že v případě distribuce takto zkopírovaných souborů na internetu nedojde k jejich přehrání. Přehrávání je možné pouze v počítači, do kterého se soubory zkopírovaly. [2]

Ochrana CDS nerespektuje „Red Book“, která obsahuje podrobné informace o standardu pro Audio CD. Ochrana je prováděna rozdělením disku na dvě sekce. První sekce je čitelná pouze přehrávači, druhá, pro změnu, zase CD-ROM mechanikou počítače. První sekce (blíže středu CD) porušuje pravidlo červené knihy, které stanovuje, že první stopa musí začínat až po dvou minutách. TOC Druhé sekce (dále od středu CD) obsahuje matoucí informace v podobě 99 zvukových stop, které začínají na místech, které se na CD ani nevyskytují. [2]

6.2 SafeAudio

Ochranu začali vyvíjet v roce 2000 izraelští TTR Technologies a Macrovision (dnešní Rovi). Hratelnost takto chráněných disků je podporována, na rozdíl od CDS, ve stejné kvalitě jak stolními přehrávači, tak počítači. Podle oficiálního vyjádření Macrovision je SafeAudio podporován výrobci EFM enkodérů, které jsou součástí všech přehrávačů. Pro uživatele je identifikace této ochrany možná až po vytvoření duplikátu, protože na přebalu disku se informace o konkrétní ochraně většinou majitel CD nedozví. [2]

Při poslechu kopie jsou patrné chyby na CD v podobě nepříjemného praskání, lupání a přeslechů. Jak už z označení plyne, měla by být zachráněna kvalita lisovaných CD při zvýšení ochrany proti nelegálnímu kopírování. Šifrované informace o chybách se dostávají na disk při samotném lisování, originální disk tedy už obsahuje tyto chyby. Rozdíl je však v tom, že je neslyšíme. [2]

Obr. 19. SafeAudio

Proti takovému postupu vystoupila v roce 2002 i společnost Philips, která uvažovala o odebrání loga CD předním výrobcům. Ti zasahují do koncepce CD, definované v roce 1978 firmami Sony a Philips. Philips potvrzuje, že ochrany CD-DA poškozují originální záznam na lisovaném CD. Nosiče s touto ochrannou technologií se už při jemném poškrábání stávají stejně nepoužitelnými jako kopie. Stává se tak, že přehrávače, které chráněné CD dříve přečetly bez problému, můžou mít při opětovném čtení problémy. [2]

7 OCHRANA DAT NA FILMOVÝCH DVD

7.1 Content Scrambling System (CSS)

Pod tímto názvem se prakticky skrývá zašifrování obsahu disku DVD, které vyžadovaly filmová studia, pro zabránění kopírování. K tomu, aby bylo možné disk spustit je potřeba znát dva klíče. Prvním je title key (klíč titulu), druhým disc key (klíč disku). Klíč titulu se nachází v hlavičce sektoru a běžným způsoben se nedá kopírovat. Na DVD se zpravidla nachází několik takových klíčů, protože každá VTS (skupina titulů) má odlišný klíč titulu. Klíč disku je umístěn v kontrolní oblasti zaváděcí stopy disku, do které rovněž není přímý přístup. [1]

Komunikace při autentizaci a dešifrování obsahu mezi mechanikou a přehrávačem (počítačem) probíhá následovně [1]:

- Mechanika i přehrávač si navzájem pošlou náhodně vygenerovaná 40 bitové čísla.
- Na čísla se aplikuje hešovací algoritmus CSS, tím vznikne číslo o délce 80 bitů (challenge key), které je zpět posláno druhému zařízení.
- To si rovněž svoje vygenerované číslo hešuje, pokud je totožné s přijatým, jedná se o zařízení z rodiny CSS.
- Mechanika se, na základě předchozích událostí, nastaví do módu umožňujícího přístup do šifrovaných oblastí.
- Na základě challenge key si obě zařízení odvodí klíč, kterým se šifruje výměna klíčů.
- Přehrávač přečte a dešifruje klíč disku, kterým dešifruje klíč titulu a dojede k přehrání.

Maximální délka symetrické šifry CSS je pouhých 40 bitů, je tedy velmi snadno a rychle prolomitelná hrubou silou. Prakticky se však jedná pouze o 16 bitů a zbylých 24 bitů je pouze jejich lineární kombinací. Šifru v roce 1999 rozšifroval, tehdy šestnáctiletý norský hacker, Jon Lech Johansen a vypustil do světa program DeCSS. [1]

CSS dále požaduje ochranu analogového signálu (APS), ochranu digitálního vysílání (DTCP) a systém regionálních kódů. [1] Všechny tyto technologie jsou řešeny dále.

7.2 Content Protection for Prerecorded Media (CPPM)

Je alternativou k CSS pro formát DVD-Audio. Může se stát, že na disku můžeme najít jak ochranu obsahu CSS, tak CPPM. V takovém případě ale musí disk obsahovat DVD-Audio i DVD-Video. Za vývojem této technologie stojí IBM, Intel, Panasonic a Thoshiba neboli skupina nazývající se 4C [1].

Ochrana funguje na principu informace obsažené v každém sektoru, která říká, zda sektor může být zkopírován. Oproti CSS neobsahuje klíč titulu ani klíč disku. Za jakousi náhradu klíče disku by se dal považovat identifikátor alba (album identifier). Identifikátor je umístěn v kontrolní části zaváděcí oblasti disku. A přesně tady nastává problém při snaze vytvoření duplikátu originálního disku. Tato oblast totiž není u disků DVD-R / RW dostupná. [1]

Počítačová DVD-ROM mechanika nebo přehrávač obsahuje 16 tajných klíčů zařízení (device keys). Na DVD se společně s identifikátorem alba vyskytuje soubor DVDAUDIO.MKB, který obsahuje matici klíčů, ta se dešifruje klíčem zařízení a získá se tak klíč média (media key). Takový klíč a identifikátor se používá pro dekódování zašifrovaných oblastí DVD. [1]

Komunikace mezi mechanikou a přehrávačem (počítačem) u CPPM probíhá takto:

- Zařízení si vymění klíče. V případě úspěšné autentizace si zařízení spočítají sběrnicový klíč pro bezpečnou šifrovanou komunikaci.
- Přehrávač (počítač) požádá mechaniku o data z kontrolní oblasti DVD. Data zašifrována sběrnicovým klíčem zašle mechanika počítači.
- Sběrnicovým klíčem počítač dešifruje identifikátor alba, kterým si následně dešifruje obsah DVD. [1]

7.3 Content Protection for Recorded Media (CPRM)

CPRM je modifikace CPPM pro zapisovatelná média DVD, SD karty a dalších flash pamětí. Každé DVD obsahuje tenký proužek u středu disku, který se nazývá Burst Cutting Area (BCA). Ten obsahuje mimo dalších informací o disku taky identifikátor média s délkou 64 bitů. Kromě identifikátoru obsahuje disk i matici klíčů (media key block - MKB), které jsou umístěné v pevně dané kontrolní oblasti disku. Stejně jako u CPPM se

tato matice zpracuje pomocí klíčů zařízení (device keys) a dojde k získání klíče média (media key). [1]

Vlastní obsah média je zašifrován jedním klíčem titulu, který se dostane na disk při zápisu. Ten je navíc zašifrován jedinečným klíčem média (media unique key). Takový jedinečný klíč média je vygenerován z matice klíčů a identifikátoru média.

Výhodou je, že matice klíčů ani identifikátor média nemusí být tajné. Důvod je ten, že při snaze vytvořit kopii disku, bude identifikátor média chybět nebo bude jiný. To povede k následnému získání jiného klíče média a disk nebude správně dešifrovatelný. [1]

Zápis na DVD chráněného CPRM probíhá takto:

- Nejdříve rekordér načte z DVD matici klíčů a svými 16 klíči zařízení z matice spočítá klíč média. Stejně tak rekordér načte identifikátor média. Z těchto dat pak vypočítá jedinečný klíč média.
- V případě, že disk ještě neobsahuje žádný klíč titulu, je náhodně vygenerován.
- Posledním krokem je samotné zašifrování dat. [1]

Aby bylo možné takový obsah přehrát, je potřeba mít zařízení, které je s touto technologií kompatibilní. Průběh dekódování je následovný (jedná se prakticky o opak zápisu na disk):

- Přehrávač načte matici klíčů, svými 16 klíči spočítá klíč média. Načte taky identifikátor média, a tím získá jedinečný klíč média.
- Následuje dešifrování klíče titulu jedinečným klíčem média.
- Posledním krokem je samozřejmě dešifrování dat klíčem titulu, tak aby jej bylo možné přehrát. [1]

7.4 Ochrana digitálního vysílání (DTCP)

Zařízení přehrávající DVD často z důvodu ochrany digitálního obsahu používá D/A převodník. Tak se zajišťuje, že digitální signál se z DVD přehrávače nedostane na jiné zařízení než na to, pro které je určeno. Aby bylo možné sledovat v digitální televizi je proto nutné, aby si televize převedla A/D převodníkem analogový signál zpět na digitální. [1]

Aby se nemusel provádět takový zbytečný proces se pětice firem (Intel, Sony, Panasonic, Hitachi a Thoshiba) podílela na vývoji DTCP. Komunikace je primárně prováděná přes

IEEE 1394 neboli FireWire rozhraní. Mezi komunikujícími zařízeními, jako je například DVD přehrávač a DVD rekordér, je vytvořen šifrovaný bezpečný kanál. Digitální data, která jsou odesílána přehrávačem, jsou šifrována a rekordér nebo digitální televize si je dešifruje. U DVD rekordérů může nastat situace, že dostanou pouze povolená data ke kopírování. Může být umožněná i kompletní kopie celého disku, ale rekordér ji musí označit identifikátorem, který zakazuje její další kopie. [1]

7.5 Rychlé digitální spojení (HDCP)

Se zvětšujícím se objemem digitálních dat a stále většími nároky na rychlost přenosu mezi počítačem a displejem rostla potřeba vytvořit univerzál pro jejich rychlé propojení, který by nahradil analogový VGA konektor. Z tohoto důvodu byla v roce 1998 vytvořena skupina DDWG (Digital Display Working Group), která se podílela na definici nové specifikace. Na jaře dalšího roku zveřejnily zakládající firmy Silicon Image, IBM, Intel, NEC, Hewlett-Packard, Fujitsu a Compaq nový standard jménem Digital Visual Interface (DVI), který umožňoval přenosovou rychlost až 4,95 Gb/s. Při porovnání s VGA, který disponuje pouze 40 Mb/s, je nárůst obrovský a umožňuje sledování videa v maximálním možném rozlišení. Aby neunikl digitální signál jinak než k displeji, bylo potřeba nový standard chránit bezpečnostním systémem, kterým je právě HDCP od Intelu. [1]

Komunikace mezi displejem a přehrávačem nebo počítačem probíhá pomocí autentizace a výměny klíčů, šifrování a rušení platnosti klíčů. Vysílač i přijímač obsahují klíče zařízení, které jsou uloženy v nepřepisovatelné paměti PROM. Autentizací se ověřuje, zda zobrazovací jednotka může přijmout zabezpečený obsah. Pro autentizaci slouží celkem 40 56 bitových tajných klíčů a vektor KVS (key-selection vector) pro jejich výběr. Vysílací zařízení odešle KVS a náhodné číslo s délkou 64 bitů. Přijímací zařízení odpoví vlastním KVS. Pokud je KVS přijímače platný, pokračuje komunikace právě na základě těchto vyměněných dat. Zařízení si spočítají klíč pro šifrování komunikace, ten je pro obě strany stejný. Autentizace se v pravidelných časových intervalech opakuje, pro případ, že by došlo k přepojení na jinou nebezpečnou linku. Samotný obsah je samozřejmě šifrován, aby při odposlouchávání linky nedošlo k pořízení pirátské kopie. [1]

7.6 Ochrana analogového signálu (APS)

Jedná se prakticky o kopii z DVD na pásku VHS. Analog Protection System (APS) chrání analogový signál pomocí obvodů od Macrovision nebo jiné společnosti, které jsou umístěny v DVD přehrávači. Na DVD je pak umístěna ke každému video souboru bitová informace o tom, zda má být použita ochrana analogového signálu a do jaké míry. V případě, že přehrávače nebo DVD-ROM mechanika neobsahuje APS, nedojde k přehrání filmu s ochranou CSS. [1]

V současnosti se kromě Macrovision uplatňuje na trhu společnost Dwight Cavendish Systems, která nabízí kompletní řešení pomocí integrovaného obvodu umístěného v Set Top Boxu. Takový obvod blokuje nahrávání na digitální rekordér a na analogový provádí, podobně jako u Macrovision, rušení obrazu. [16]

7.7 Chybné sektory

Technologie, spočívající v umístění vadných datových sektorů na disk. Standardní software pro kopírování, jako je například nejrozšířenější Nero, se úmyslně porušené sektory snaží opravit a v případě, že se mu to nepodaří, tak kopírování selže. Existují i programy, které si s přeskakováním chybných sektorů poradí, ale ani tady není úspěch vytvoření stoprocentně funkční kopie zaručený. [15]

Mezi takový způsob řešení patří mimo jiné ARccOS, DVD-R-Movie PROTECT nebo FluxDVD. ARccOS od společnosti Sony se, díky napadnutelnosti mnoha softwarovými programy, už údajně nepoužívá. DVD-R-Movie PROTECT od X-protect a FluxDVD od ACE GmbH má zase problémy s kompatibilitou a nerušeným přehráváním filmu. [15]

7.8 Změna obsahu

Pozměnění obsahu si klade jako cíl znemožnit použití softwarových produktů na obcházení a zneškodnění ochrany, při udržení maximální kompatibility s přehrávači. Mezi takové ochranné technologie patří taky RipGuard od Macrovision, představený poprvé v únoru roku 2005. Pravdou je, že s určitými znalostmi a patřičným programem, jako je AnyDVD nebo DVDFab, jde ochranu obejít. [15]

Další společností, která se věnuje právě změnou obsahu disku, je Rimage se svým Rimage Video Protect. Takové softwarové řešení vychází z umístění datových souboru na určitá

místa DVD. Pozitivem je, že na rozdíl od chybných sektorů se nedegraduje záznam videa, protože takové datové soubory nejsou vůbec během přehrávání disku načítány. Původní obsah je tudíž nezměněn a vysoká kompatibilita s přehrávači zachována. [15]

7.9 Systém pro správu kopírování (CGMS)

Kopírování nemusí být omezeno striktně pro všechny, proto existuje Copy Generation Management System (CGMS), který nám dává možnosti vytvoření pouze kopie originálu, kopie z kopie nebo naprosto kopírování zakazuje. Prakticky je správa ošetřena dvěma příznakovými bity, jejichž kombinace udává tyto možnosti. Všechna zařízení ale takové informace nemusí respektovat a tudíž může dojít i k vytvoření kopie tam, kde by to nemělo být možné. [1]

7.10 Regionální kódy

Regionální kód není stejně jako CGMS žádná šifra, jedná se pouze o několik bitů, které jsou přehrávačem kontrolovány. Pokud přehrávač podporuje region, tak DVD přehraje. Celý svět je v rámci regionálních kódů rozdělen na šest regionů. Rozdělení nevychází ze specifikace DVD. Důvod nasazení těchto kódů je ryze obchodní. Regionální kód je opatření proti přenášení DVD z jedné oblasti do druhé. Rovněž je důvodem udržení smluv s místními distributory. Přehrávače i mechaniky však mnohdy disponují více než jedním regionem a umožňují i jejich změnu. [5]

7.11 Vodoznaky

Stejně jako vodoznaky na papírových cennostech, tak i vodoznaky na filmových DVD patří mezi technologii, která dokáže bojovat proti kopírování. Vodoznak nechrání obsah přímo, tedy neznemožňuje vytvořit kopii. Umožňuje snadnou identifikaci nelegální kopie i po konverzi videa. Vodoznaky jsou vkládány do videa tak, aby nebyly snadno identifikovatelné. I když se výrobci vodoznaku hájí tím, že vodoznaky nedegradují žádným způsobem kvalitu obrazu, tak názory jiných expertů v oblasti jsou, že se v obrazu projevuje více šumu než obvykle. Informace obsažené ve vodoznaku obsahují zpravidla čas, datum, místo a taky možnost sledování pirátské kopie až k distributorovi, a tím tak odhalovat tohle protiprávní jednání. Princip takových vodoznaků si výrobci pochopitelně patřičně chrání. Patří zde technologie jako RUNNING MARKS, VTrack, VideoMark nebo NexGuard. [15]

8 OCHRANA DAT NA BLU-RAY DISCÍCH

S příchodem videa ve vysokém rozlišení si musel být Hollywood jistý, že nová generace optických disků spolehlivě ochrání jejich obsah před vytvářením kvalitních digitálních duplikátů.

Podobně jako u DVD můžeme rozdělit principielně ochrany kopírování Blu-ray na čtyři skupiny:

- Ochrana vysílání: Ochrana digitálního vysílání (DTCP) a ochrana rychlého digitálního spojení (HDCP). Tyto ochrany jsou u Blu-ray naprosto totožné jako u DVD.
- Povinná ochrana před vytvoření přímé kopie disku: Zde se jedná, v porovnání s DVD, o značné vylepšení. Místo CSS a CPPM nastupuje systém AACS a doplňuje ho BD-ROM Mark.
- Komerční ochrana před vytvoření přímé kopie disku: Ochrana technologie BD+.
- Doplňkové mechanismy: Regionální kódy a vodoznaky, prakticky přejaté z DVD. V souvislosti s BD+ bývá s oblibou používán vodoznak NexGuard.

Stejně jako u ochran předešlých typů médií, je nutné při vývoji ochrany respektovat technologické, obchodní i právní hledisko. Technologie definuje, jakým šifrováním popřípadě vodoznaky se bude disk chránit, aby se zabránilo vytvoření digitální kopie. Z obchodního hlediska musí být tato technologie respektována výrobci přehrávačů a mechanik, aby nedošlo ke konfliktu mezi ochranou na disku a zařízením. Nemluvě o ceně, kterou je ochoten zákazník za Blu-ray disk i přehrávač zaplatit. A z hlediska právního musí být v zákoně ošetřena vymahatelnost náhrady škod, pokud dojde k porušení příslušných zákonů. [8]

8.1 Advanced Access Content System (AACS)

AACS je hlavní ochrana, která se objevila u Blu-ray a u každého disku je povinná. AACS je vylepšená ochrana, vycházející z CSS a CPPM, které se používají u DVD. Na jejím vývoji se podílely společnosti IBM, Intel, Microsoft, Panasonic, Sony, Toshiba, Walt Disney a Warner Bros. [8]

AACS využívá šifru AES s délkou klíče 128 bitů. Podobně jako u CPPM a CPRM, které se prokázala u DVD jako poměrně spolehlivá, se i zde využívá technologie Media Key Block (MKB). Dešifrování obsahu disku je naprosto totožné jako u předešlé generace. Licenční autorita poskytuje pro každé zařízení sadu klíčů (device keys). Každý disk je opatřený maticí klíčů. Pokud jsou obě komunikující strany kompatibilní, tak si přehrávač vypočítá klíč média (media key), kterým se dešifruje klíč titulu (title key), a tím následně obsah audio a video souborů na disku. [8]

Novinkou u AACS je umožnění uživateli vytvořit si kopii disku před jeho přehráním například na domácí server nebo do přehrávače v automobilu. Nutná je ale podpora AACS veškerými zařízeními, které mají takový přesun provádět. Takovou správu kopírování řeší právě AACS Managed Copy. Ten umožňuje, kromě mnohem tvárnější správy kopírování, postahovat z Internetu další bonusové a jiné materiály. Informace o právech majitele BD-ROM jsou uvedeny právě na disku v jeho Burst Cutting Area (BCA) pomocí jedinečného identifikátoru Prerecorded Media Serial Number (PMSN). [8]

Ochrana obsahu AACS je dostupná i pro zapisovatelná média. Nutností je však mít potřebnou licenci, připojeni na Prepared Video Authorization Server (PVAS) pro získávání klíčů a samozřejmě rekordér s podporou této technologie. [8]

8.2 BD-ROM Mark

Společně s AACS tvoří povinnou výbavu každého Blu-ray disku i BD-ROM Mark. Jedná se prakticky o to, že na přehrávačích půjdou přehrát pouze BD-ROM s tímto vodotiskem. Vytvoření kopie bez sebemenších problémů tak neznamená, že po vložení disku do přehrávače uvidíme samotný film. Pro výrobu Blu-ray se používá přístroje jménem BD-ROM Mark Inserter, který mají jen licencovaní výrobci BD-ROM s přísnými nároky na bezpečnost celého procesu. Další výhodu této technologie je výhoda sledování v případě nalezení pirátských kopií disků za pomocí 128 bitového klíče pod názvem Volume ID, který je důležitý taky pro úspěšné dešifrování média. [8]

8.3 BD+

Technologie BD+ pracuje na principu virtuálního stroje (Security Virtual Machine, SVM), který je v každém BD-ROM přehrávači, aby bylo možno převést úmyslně poškozené BD+

data do podoby kvalitního video a audio signálu. Virtuální stroj je spouštěn pouze v případě detekce ochrany BD+. Při nelegálním zkopírování disku z tuhle ochranou bez speciálních pomůcek na její odstranění, se bude film trhat, až se úplně zasekne. BD+ Technologies LLC, která se stará o udělování licencí na BD+ se pochopitelně k detailnímu popisu technologie nestavěla příliš otevřeně, přesto se už v roce 2008 podařilo společnosti SlySoft ochranu zdárně prolomit. [8]

8.4 Blu-ray regiony

Blu-ray, stejně jako DVD-Video, disponuje rozdělením světa na regiony, a tak částečným omezením přenášení Blu-ray nosičů mezi nimi. Ve srovnání s DVD však disponují pouze třemi oblastmi:

- Region A: Amerika, Korea, Japonsko, jihovýchodní Asie
- Region B: Evropa, Střední Východ, Afrika, Austrálie, Nový Zéland
- Region C: Rusko, Indie, lidová republika Číny, zbytek světa [8]

Obr. 20. Blu-ray regiony [8]

Regionální kódy na Blu-ray už nejsou tak frekventované jako na DVD. Většina disků tak podporuje všechny regiony.

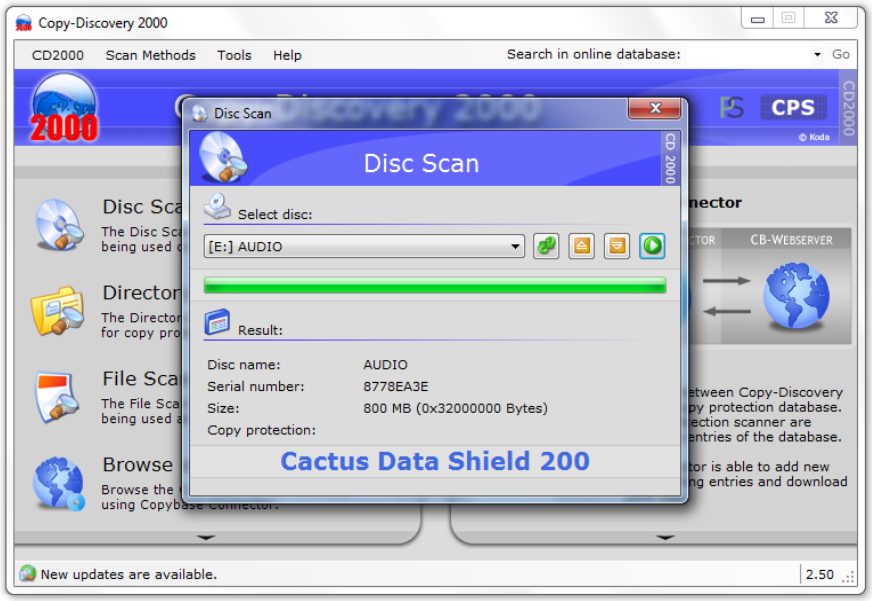
II. PRAKTICKÁ ČÁST

9 DETEKČNÍ A DEAKTIVAČNÍ SOFTWARE

Předmětem této kapitoly jsou pouze běžně dostupné programy, které nepodléhají placení licencí ani registrování. Jedná se tedy buď o programy distribuované bezplatně (freeware), nebo o programy distribuované volně s určitou dobou bezplatného fungování (shareware).

9.1 Software na identifikaci ochrany

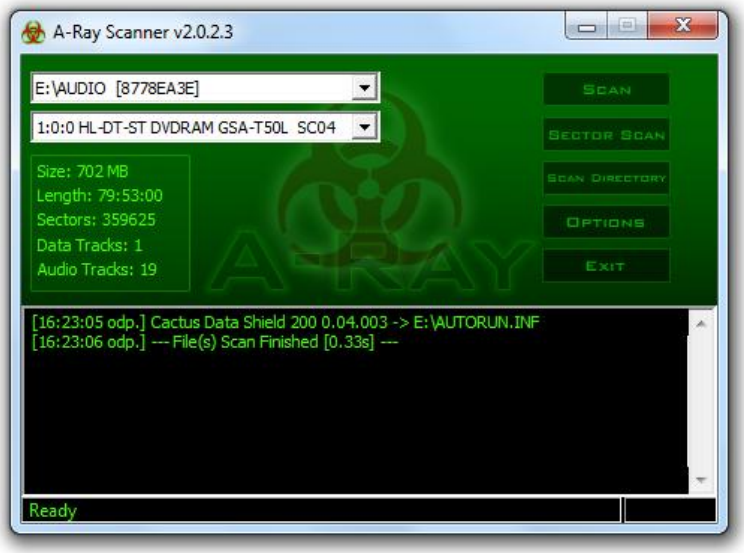
Je prakticky nemožné rozpoznat ochranu na disku pouhým pohledem, moc informací o ní nepodá ani průzkumník ve Windows, který slouží jako základní nástroj systému pro manipulaci a prohlížení souborů. Proto na rozpoznání ochrany proti kopírování existují softwarové nástroje, které disk analyzují a poskytnou informace o tom, jaká ochrana je na disku skutečně implementována. Mezi takové programy se dají zařadit především A-Ray Scanner nebo Copy-Discovery 2000.



Obr. 21. Nalezení ochrany CDS 200 pomocí Copy-Discovery 2000

Copy-Discovery 2000 je jednoduchý program s intuitivním ovládáním, který umožňuje kontrolovat nejen disky, ale i adresáře a jednotlivé soubory na přítomnost ochrany proti kopírování. Součástí je i přístup do online databáze ochran Copybase a možnost vkládání vlastních informací o druhu používaných ochran u konkrétních disků. A-Ray Scanner obsahuje test média na přítomnost ochrany. Tlačítka na rozpoznání ochrany fungují prakticky stejně, „Sector Scan“ zjistí název ochrany, kdežto „Scan“ i její případnou verzi.

Stejně jako u Copy-Discovery 2000 je možnost testování adresáře na pevném disku či jiném datovém médiu. Oba programy umožňují provádět aktualizace databáze, které jsou pro správné detekování ochrany velmi důležité.



Obr. 22. Detekce CDS 200 programem A-Ray Scanner

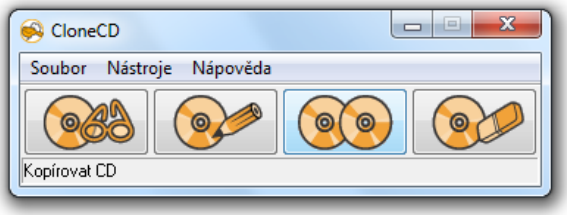
Oba výše testované programy jsou dostupné v licenci freeware, takže si je každý může zdarma vyzkoušet. Aby bylo možné provést účinnou a spolehlivou detekci ochrany, je třeba mít co nejaktuálnější software, který je takovou ochranu schopen rozpoznat. A-Ray Scanner 2.0.3.3 i Copy-Discovery 2000 2.50 jsou schopni rozpoznat až 26 ochran používaných jak u CD, tak u DVD, rozdíl je však ve skladbě rozpoznávaných ochran. Proto není možné jednoznačně říct, který z nich je účinnější. Pro porovnání je dobré se ohlédnout zpátky do roku 2000, kde skončil vývoj programů Protection Detective nebo CD Protection Scout, oba tak detekují pouze osm ochran. Nemělo by být zapomenuto ani na poslední verzi ClonyXXL z roku 2003, která podporovala celkem třináct ochran.

Další možností, jak zjistit jaká ochrana se na disku vyskytuje, je pomocí webových stránek. Jedna je přímo na stránkách výrobce DAEMON Tools. Konkrétně se jedné o stránku na fóru s adresou *http://forum.daemon-tools.cc/gamedb.php,* kde se nachází seznam většiny populárních i méně populárních her a informace o jejich ochranách proti kopírování. Další možnou alternativou je švýcarská stránka Copybase dostupná z adresy *http://copybase.org/en/database/.*

9.2 Software umožňující vytváření kopie chráněného disku

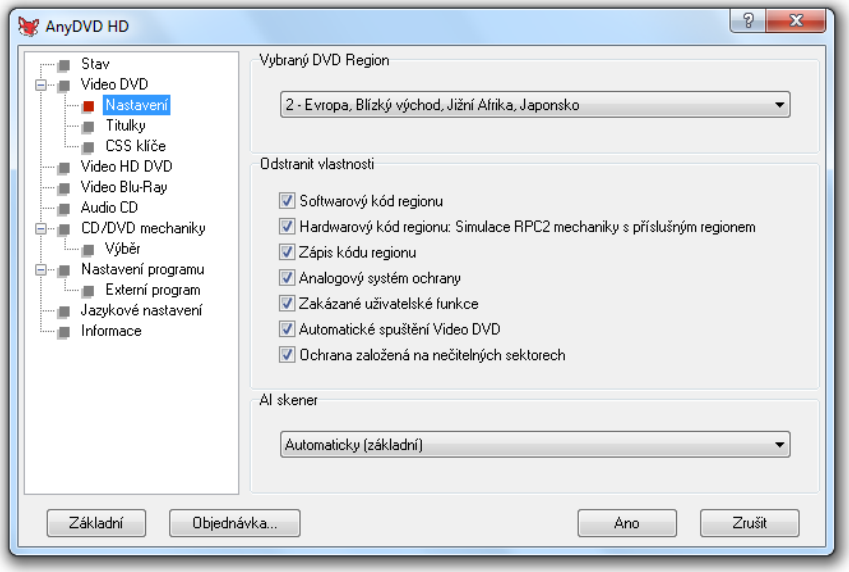
Produktů, které slouží k obcházení ochranných technologií je spousta, proto bude zmínka pouze o majoritních a nejvíce oblíbených. Kompletní řešení pro kopírování chráněných CD, DVD i Blu-Ray disků poskytuje výrobci ochran společnost SlySoft [20]. Prvním jejich produktem je CloneCD.

CloneCD umožňuje kopírovat jak datové, tak hudební CD. Od verze 5.0 umožňuje kopírovat i DVD. Ke kopírování filmových DVD se ale používá především CloneDVD a AnyDVD. CloneCD je první software, který využívá RAW-mode, vytváří tedy přesnou 1:1 kopii pomocí zesílení a emulace slabých sektorů.



Obr. 23. CloneCD

Dalším produktem z dílny SlySoft je CloneDVD a AnyDVD. CloneDVD sám o sobě nefunguje jako nástroj pro kopírování chráněných disků. Pouze umožňuje zkopírovat vybrané video a zvukové souboru z filmového DVD. Aby bylo možné kopírovat i zabezpečené filmy, je potřeba spolupráce s programem AnyDVD, který se postará o úmyslné chyby tvořené při masteringu, odstranění ochrany CSS, regionálního kódu i analogové ochrany signálu Macrovision na pozadí a to ihned při vložení každého disku do mechaniky. Současně umožňuje AnyDVD i dešifrování chráněných audio CD.



Obr. 24. AnyDVD

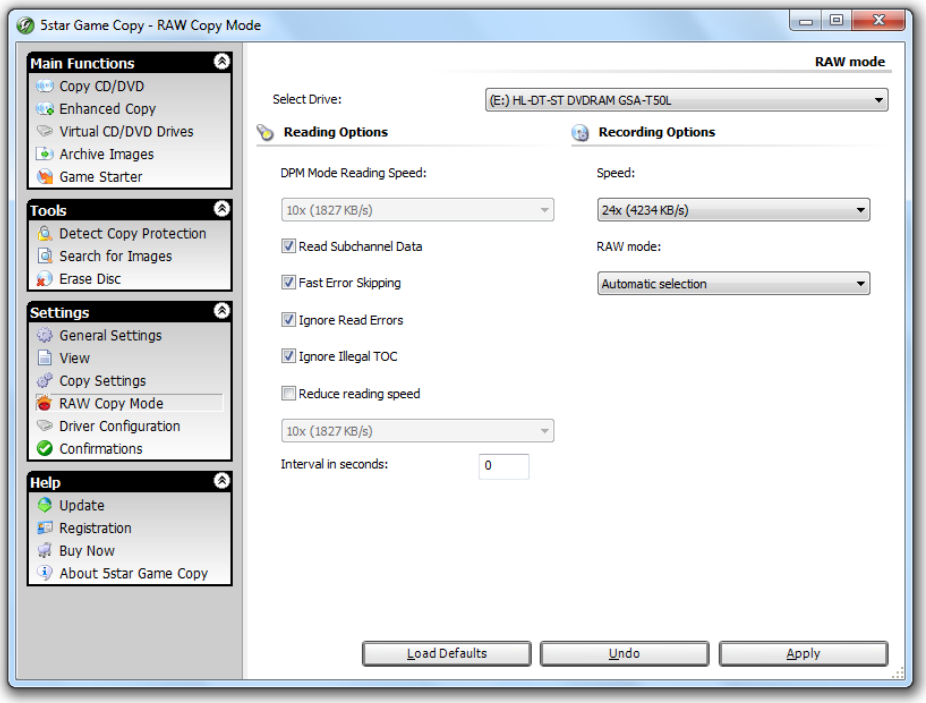
AnyDVD podporuje rovněž kopie Blu-ray i HD DVD, proto jeho dnešní verze nese označení AnyDVD HD. Z Blu-ray disku odstraní kódování AACS, ochranu BD+ i regiony. Aby toho nebylo málo, umožňuje sledování videa i bez kompatibilní grafické karty a displeje s technologií HDCP.

Bohaté nastavení pro kopírování chráněného DVD s filmem obsahuje i volně šiřitelný program DVD Decrypter, který podobně jako CloneDVD disponuje odstraněním ochrany CSS, regionu, pracuje s vadnými sektory, umožňuje vynechat nepřeskočitelné kapitoly nebo odstranit ochranu analogového signálu od Macrovision.

Poslední z rodiny SlySoft „Herní šakal“ je jediný produkt na trhu, který umožňuje hrát chráněnou počítačovou hru na počítači bez nutnosti image souboru a přítomnosti zdrojového disku v mechanice. Image souboru je diskový obraz což je soubor obsahující digitální kopii dat disku, který mimo datových souborů obsahuje i obraz všech metadat souborového systému, včetně Boot sektoru a atributů. Pomocí programu Game Jackal se pouze vybere zdrojová jednotka a hra se nakopíruje pomocí speciálního průvodce několika kliknutími na disk.

Software 5star Game Copy od německé společnosti Engelmann Media GmbH patří mezi hráči počítačových her k hodně oblíbeným. Poradí si i s CD a DVD se kterými ostatní programy ne. 5star Game Copy má intuitivní ovládání a chytré technologie, které se například mimo ochran StarForce poradí i s kopií dvouvrstvého DVD. Prakticky se jedná o

jakýsi komplet, který obsahuje detekci ochrany, vytvoření kopie i virtuální jednotky pro emulaci image souborů.



Obr. 25. 5star Game Copy

Po přečtení této kapitoly by čtenáře mohla napadnout otázka, jestli je vývoj a distribuce takových aplikací vůbec v souladu se zákonem. U produktů SlySoft je právní otázka věci řešená tím, že společnost má sídlo v Karibiku na ostrově Antigua, kde neplatí americké ani evropské zákony, takže může beztrestně vyvíjet a nabízet takové programy. V Německu je zase situace vyplývající ze zákona sporná, proto Engelmann Media GmbH může prodávat takovýto software. Podobně i u DVD Decrypteru se dostávají výrobci do konfliktu s distributory filmů.

Právní možnosti vytváření kopií chráněných médií v České Republice jsou podrobně řešeny v poslední kapitole této práce.

10 VÝROBA CHRÁNĚNÉHO DISKU POMOCÍ NERO SECURDISC

Výše byly představeny ochrany proti kopírování, jejich nalezení i možnosti úspěšné deaktivace, nyní se budeme zabývat prostředky zaměřenými na ochranu vlastních dat na CD, DVD nebo Blu-ray discích proti jejich zneužití.

Protože je tato kapitola určená pro široké spektrum uživatelů, byl kladen důraz především na dostupnost a rozšířenost testovaného produktu. Tím tedy není nic jiného než vypalovací program jménem Nero, který je možno během prvních 15 dnů testovat zcela zdarma.

Obr. 26. SecurDisc

Nero se podílelo na vývoji technologie SecurDisc [21] společně s LG a v roce 2007 ji implementovalo do programu Nero Express. Až do roku 2010 se tradovalo, že se jedná o kombinaci hardwarové a softwarové ochrany. LG tedy byla jediná společnost, která prodávala mechaniky podporující tuto technologii. Od 12. dubna 2010 ale SecurDisc 2.0, v balíku jménem Nero 10 Multimedia Suite, funguje prakticky na jakékoliv mechanice.

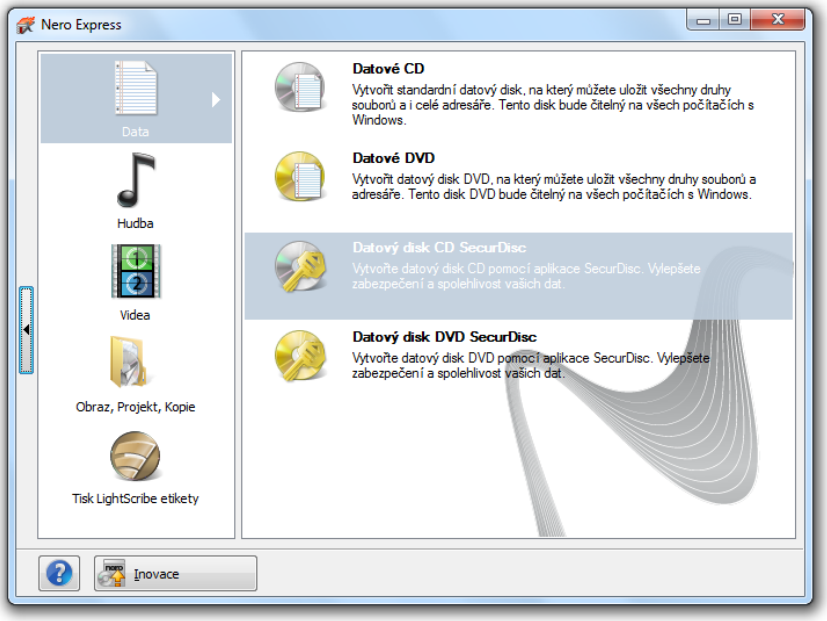
SecurDisc 2.0 obsahuje:

- Ochranu proti neoprávněnému přístupu: Šifrování dat 128 bitovou šifrou AES, přístup je povolen pouze v případě zadání hesla.
- Ochranu před manipulací s obsahem: Zabezpečení obsahu pomocí digitálního podpisu s využitím veřejného a soukromého klíče.
- Kontrolu čitelnosti dat, v případě, že jsou už hůře čitelná, zobrazí varování, že by se měly zálohovat na jiný disk.
- Lepší čitelnost poškrábaných disků díky vkládání dalších duplicitních údajů pro případ poškození.

Pochopitelně bude předmětem práce pouze opatření heslem a zabezpečení digitálním podpisem, které lze i kombinovat.

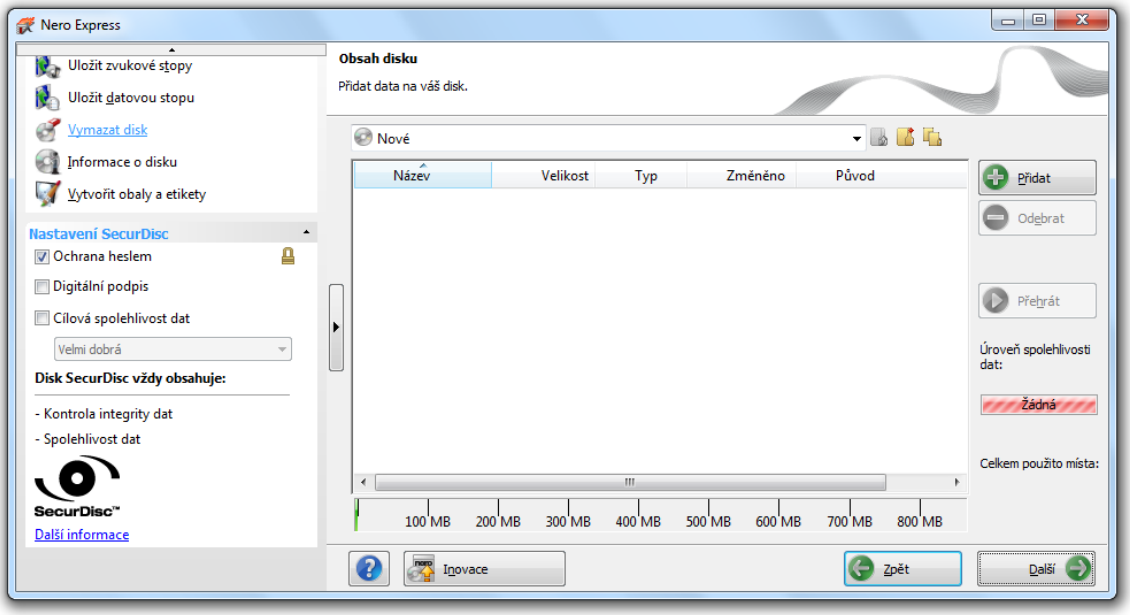
10.1 Ochrana heslem SecurDisc

Pro tvorbu datového disku opatřeného SecurDisc 2.0 je třeba spustit Nero Express a vybrat „Datový disk CD/DVD/Blu-ray SecurDisc“.

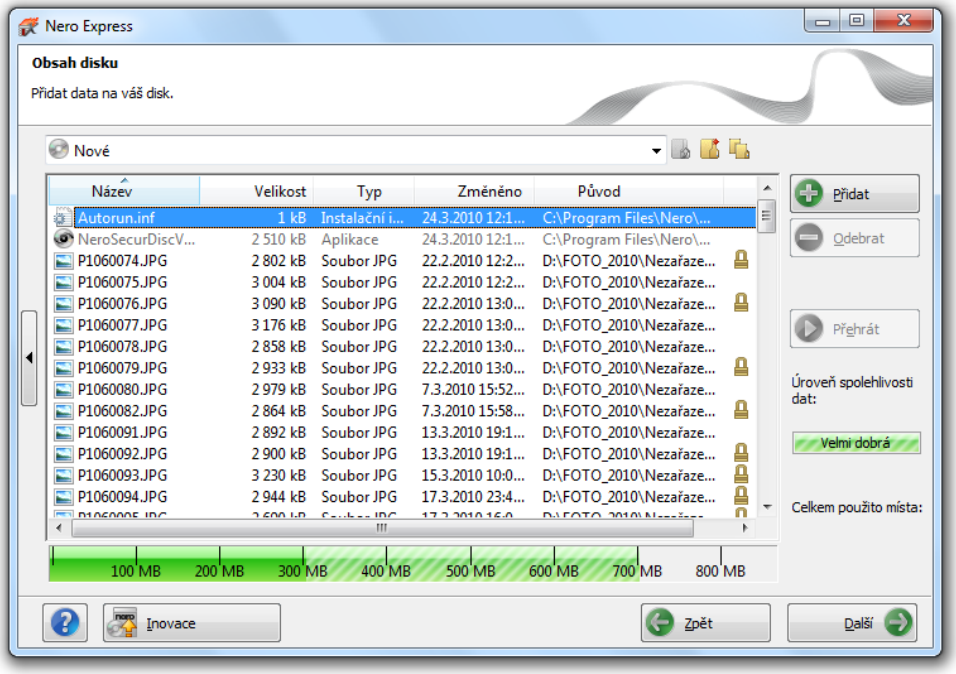


Obr. 27. Tvorba CD chráněného heslem (krok 1)

Po zvolení datového disku SecurDisc a kliknutí na šipku v levé části okna, se rozbalí rozšířená nabídka s nastavením, kde je třeba zaškrtnout „ochrana heslem“.



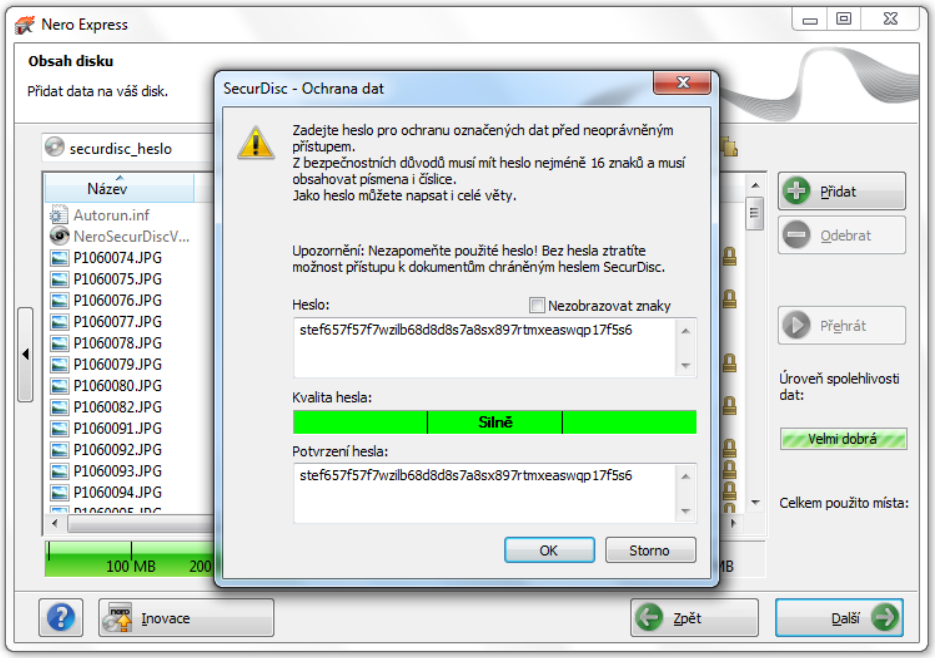
Obr. 28. Tvorba CD chráněného heslem (krok 2)



Obr. 29. Tvorba CD chráněného heslem (krok 3)

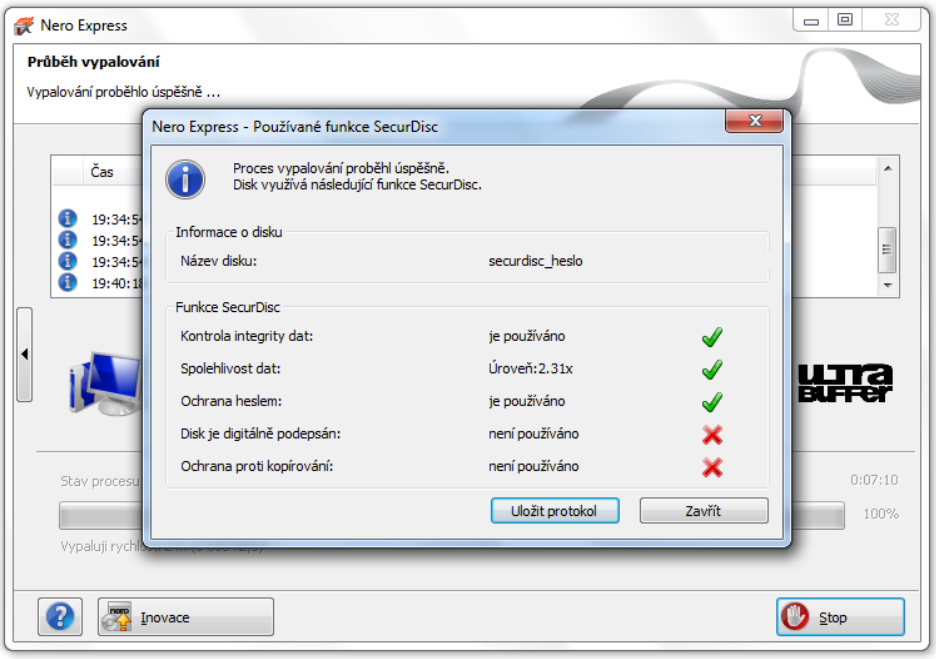
Automaticky se šifrují všechny soubory přidávané do kompilace. Jak je ale vidět, u některých souborů na obrázku zámek není. SecurDisc totiž umožňuje vybrání těch souborů, které chceme mít přístupné bez hesla a těch, které pouze s heslem.

Po klepnutí myší na tlačítko „Další“ je tvůrce disku vyzván k zadání hesla, jehož kvalita je vizuálně odstupňována. Následně stačí vložit do vypalovací mechaniky pouze jakékoliv prázdné CD a počkat až se kompilace vypálí.



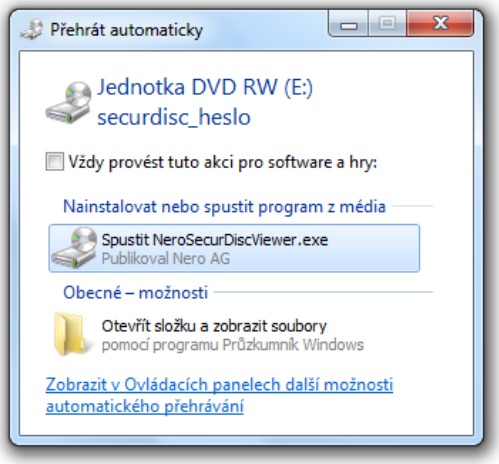
Obr. 30. Tvorba CD chráněného heslem (krok 4)

Po dokončení vypalování je zobrazeno, jaké funkce SecurDisc jsou využívány.



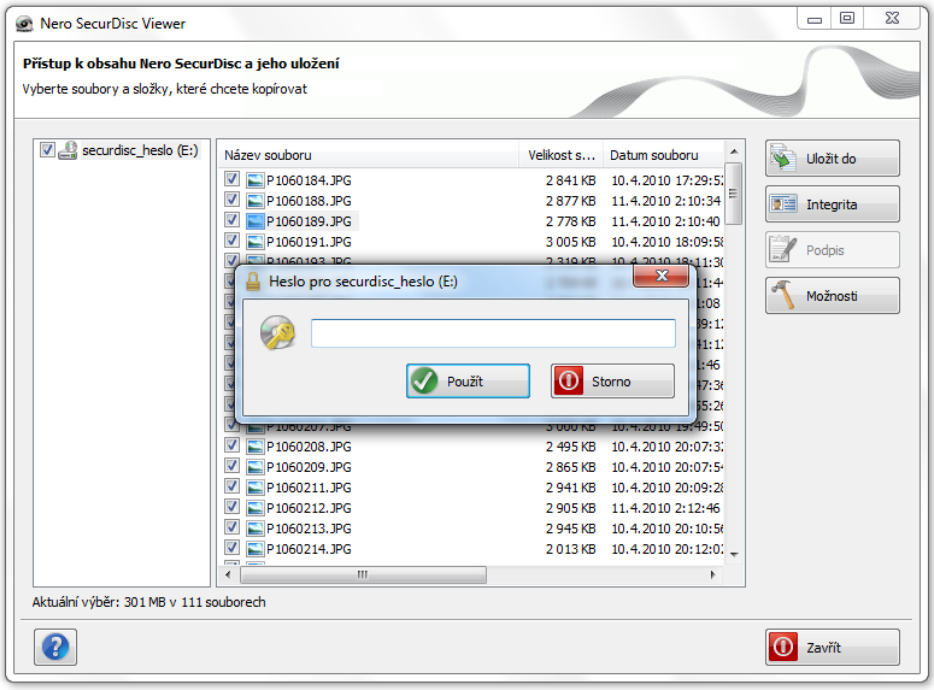
Obr. 31. Tvorba CD chráněného heslem (krok 5)

Při vložení vypáleného CD do mechaniky, je po jeho načtení zobrazena nabídka, ve které se vyskytuje i spuštění programu Nero SecurDisc Viewer.



Obr. 32. Spuštění chráněného CD

Přes tento program dochází tlačítkem „Uložit do“ právě k rozbalování chráněných souborů, prostřednictvím zadání hesla zvoleného při pálení.



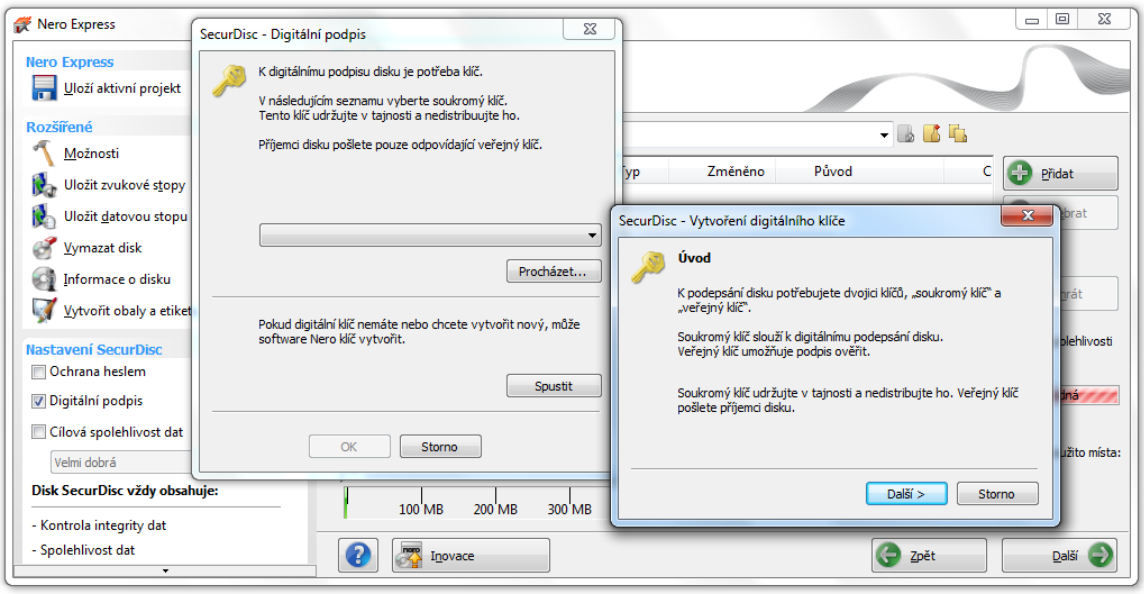
Obr. 33. Otevírání chráněného CD programem Nero SecurDisc Viewer

Jak lze vidět na obrázku, v pravé části okna není aktivní jedno tlačítko s názvem „Podpis“, protože CD není opatřeno digitálním podpisem.

10.2 Digitální podpis SecurDisc

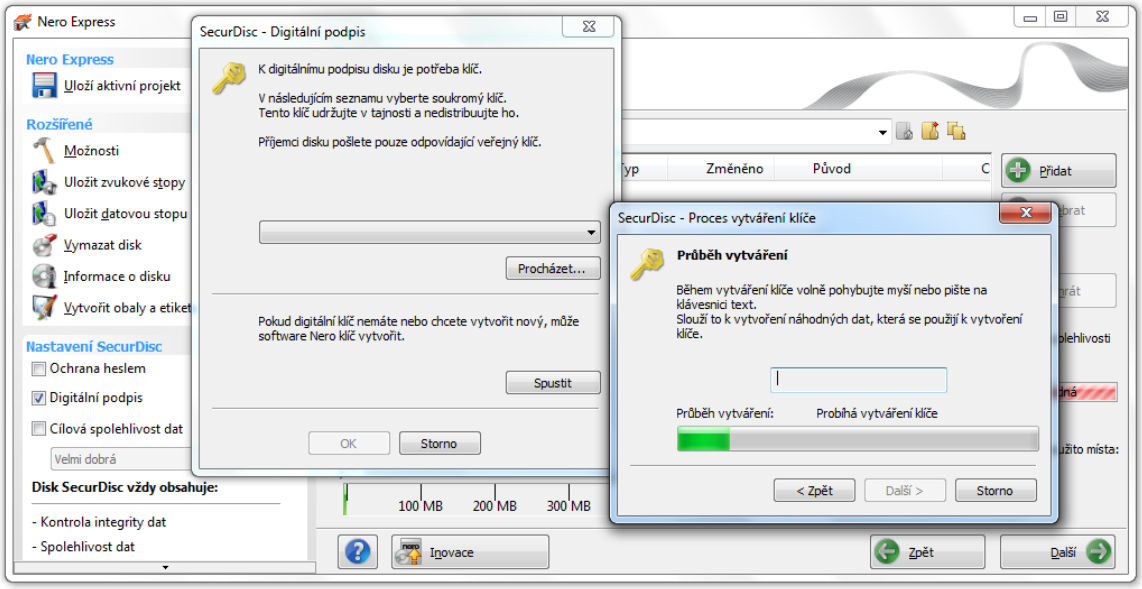
Digitální podpis nefunguje jako nástroj k zamezení kopírování ani k zamezení přístupu jako v případě opatření heslem. Při vypalování je vygenerován soukromý a veřejný klíč. Data jsou při vypalování zašifrována soukromým klíčem. Člověk, který získá vypálené CD, si ověří pravost média pomocí veřejného klíče, který mu poskytne autor kompilace.

Po spuštění Nero Express a výběru disku opatřeného SecurDisc, stejně jako v případě opatření heslem, se vybere v nastavení v levé části „Digitální podpis“. Ihned po jeho aktivaci je tvůrce kompilace vyzván k zadání soukromého klíče. Pokud není ještě ani jeden vygenerován, musí se vytvořit kliknutím na tlačítko „Spustit“. Vyskočí další okno, kde je třeba kliknout na „Další“.



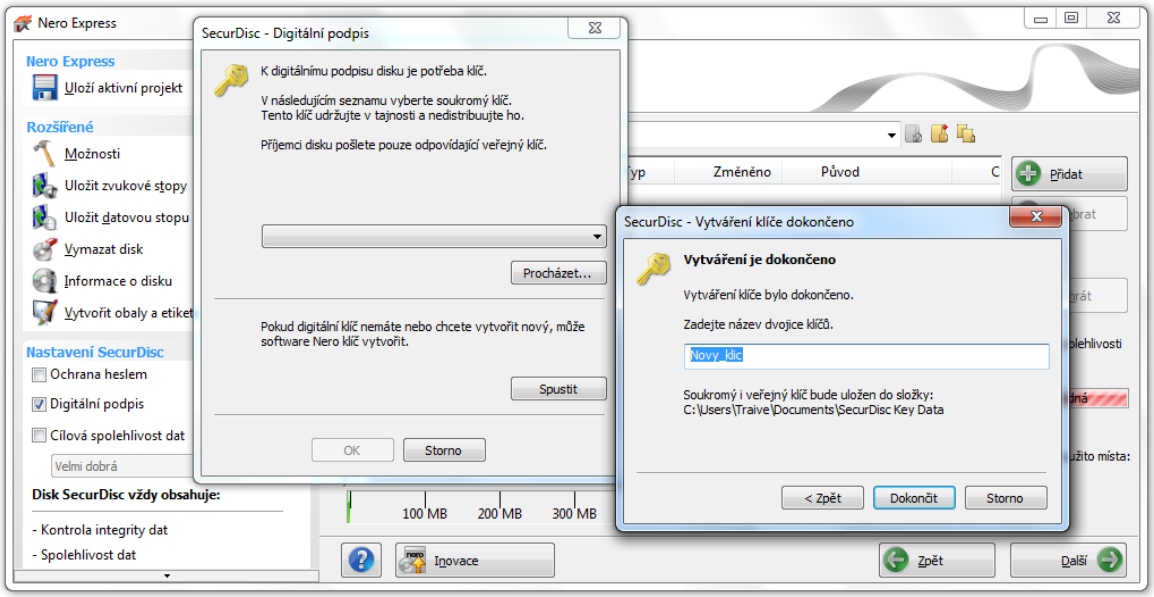
Obr. 34. Tvorba CD s digitálním podpisem (krok 1)

Proto, aby se mohl vygenerovat klíč je potřeba pohybovat myší nebo psát libovolný text na klávesnici. Takový postup je používán prakticky při generování jakýchkoliv digitálních podpisů (například na elektronické podepisování dokumentů).



Obr. 35. Tvorba CD s digitálním podpisem (krok 2)

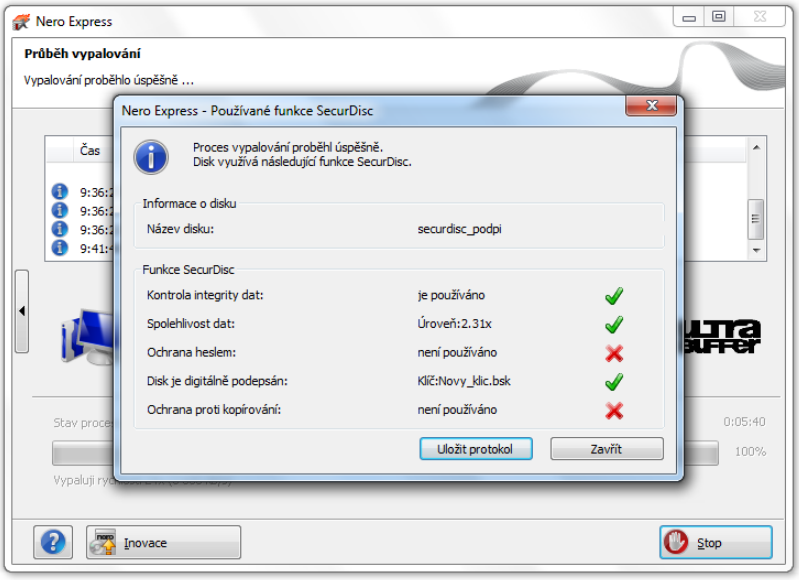
Až se tvorba klíče dokončí, stačí už jen potvrdit otevřené okna, přidat na CD soubory a vypálit jej.



Obr. 36. Tvorba CD s digitálním podpisem (krok 3)

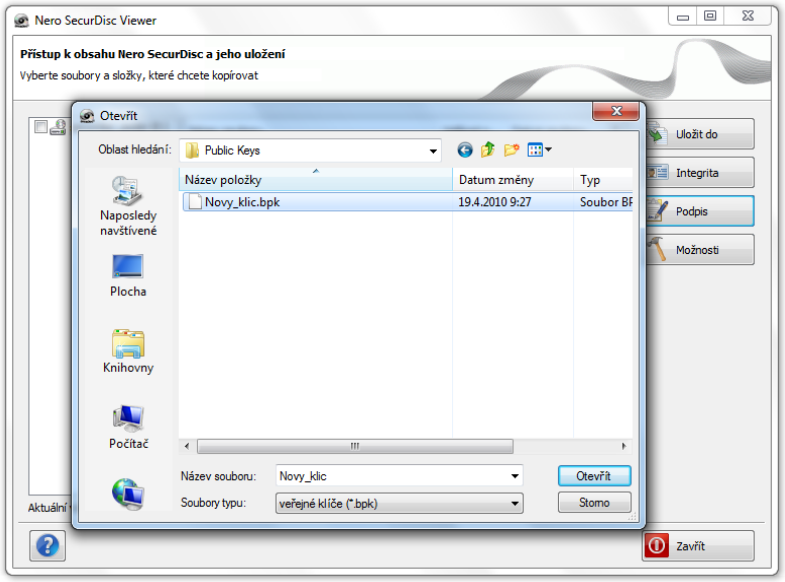
Po dokončení vypalování bude opět zobrazen souhrn funkcí SecurDisc, které se na vypáleném disku vyskytují. Možná by se někdo mohl pozastavit nad položkou „Ochrana proti kopírování“, kde je napsáno „není používáno“. Onou ochranou je myšlena ochrana speciálně pro dokumenty PDF, která u testované vypalovací mechaniky nebyla ani

v nabídce. Při testování vypalování na mechanice značky LG však tato volba nastavení SecurDisc viditelná byla a mohla být použita. Je tedy možné, že ochrana kopírování PDF souborů funguje pouze pro vypalovací mechaniky značky LG, které mají jakousi hardwarovou výhodu.



Obr. 37. Tvorba CD s digitálním podpisem (krok 4)

Po spuštění CD pomocí programu Nero SecurDisc Viewer je aktivní už i tlačítko „Podpis“. Pokud chce vlastník ověřit pravost média, stačí kliknout na „Podpis“ a vybrat veřejný klíč obdržený od tvůrce CD.



Obr. 38. Vybrání veřejného klíče k ověření CD

10.3 Test odolnosti technologie SecurDisc vůči kopírování

Při srovnání testované technologie s ochranami, které jsou uvedeny na začátku této práce, založenými především na překažení kopírování disku, nebude žádný problém nosič se SecurDisc zkopírovat. Neobsahují totiž žádné nečitelné sektory. V případě ochrany heslem nastane problém až přístupem k chráněným datům. Informace se tak z disku nedostanou k nežádaným osobám i v případě, že se jim dostane do rukou takto chráněný datový nosič. Tyto informace byly potvrzeny praktickým testováním výskytu ochrany proti kopírování programem A-Ray Scanner a Copy-Discovery 2000. Ani jeden z nich, dle předpokladů, nic nenašel, tudíž nebyl problém disk zkopírovat programem Nero, v kterém byl původně vytvořen. Aby nebylo testování kopírování závislé pouze na jednom výsledku, bylo provedeno i v programu CloneCD a to rovněž s úspěchem.

CD, DVD nebo Blu-ray opatřený digitálním podpisem lze rovněž, podle vlastního testování, libovolně kopírovat bez vlivu na schopnost verifikace digitálního podpisu. Stejně tak není digitální podpis detekován A-Ray Scanner ani Copy-Discovery 2000. Problém s ověřením by nastal v případě, že by se někdo snažil manipulovat se soubory a vypálit je v aplikaci Nero jako SecurDisc, ten by měl jiný podpis a verifikace by zahlásila chybu.

Nevýhodou zabezpečování obsahu heslem je především nutnost otevírání obsahu disku přes speciální program SecurDisc Viewer a jeho následné rozbalování, čímž se na úkor zvýšení bezpečnosti zvyšuje i čas, který vede k oprávněnému přístupu k uloženým datům. Pokud je optický disk opatřen pouze digitálním podpisem, je možné procházet a kopírovat jednotlivé soubory (např. fotografie) i pomocí průzkumníka Windows. Program SecurDisc Viewer je zde využitý pouze jako ověření, zda médium, které se nám dostalo do rukou, není nijak upravováno.

11 PRÁVNÍ STRÁNKA VĚCI

11.1 Legislativní prostředky České Republiky

Tvoření zákonů nebo jejich úprava byla vždycky odpovědí na určité změny ve společnosti. Autorský zákon č. 121/2000 Sb. definuje právní možnosti jak producentů, tak uživatelů. Trestní zákoník č. 40/2009 Sb. pak definuje konkrétní sankce za porušení pravidel uvedených v autorském zákonu. Těmito zákony je nezbytné se řídit při jakékoliv manipulaci s chráněnými daty, které jsou předmětem této práce. Proto je nutností se s autorským zákonem, definující mimo jiné tzv. účinné technické prostředky ochrany práv a volná užití, seznámit. [6]

11.2 Autorský zákon

§ 30 Volná užití

„(1) Za užití díla podle tohoto zákona se nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak.

(2) Do práva autorského tak nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.

(3) Nestanoví-li tento zákon dále jinak, užitím podle tohoto zákona je užití počítačového programu či elektronické databáze i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu; stejně je užitím podle tohoto zákona zhotovení rozmnoženiny či napodobeniny díla architektonického stavbou i pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby (§ 30a) a pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu (§ 20) i pro osobní potřebu fyzické osoby.

(4) Rozmnoženina nebo napodobenina díla výtvarného zhotovená pro osobní potřebu fyzické osoby podle odstavce 1 musí být jako taková vždy zřetelně označena.

(5) Rozmnoženina nebo napodobenina díla výtvarného zhotovená pro osobní potřebu fyzické osoby podle odstavce 1 nesmí být použita k jinému než tam uvedenému účelu.

(6) Ustanovení § 25, 43 a 44 nejsou odstavcem 1 dotčena.“ [6]

V autorském zákonu je tedy jasně napsáno, že právo na vytvoření kopie máme, ale musíme splňovat určité podmínky. V § 30 je ve zkratce uvedeno že, kopie musí být pouze pro vlastní použití. Jakékoliv darování, půjčení nebo veřejná projekce je klasifikována jako protiprávní jednání. Po přečtení tohoto paragrafu by se mohlo zdát, že si prakticky můžeme zkopírovat jakékoliv vlastní originální CD nebo DVD, pokud je vytvořený duplikát pouze pro naši osobní potřebu. Není tomu ale úplně tak. Nesmíme totiž obejít účinné technické prostředky ochrany práv uvedené v § 43. [6]

§ 43 Účinné technické prostředky ochrany práv

„(1) Do práva autorského neoprávněně zasahuje ten, kdo obchází účinné technické prostředky ochrany práv podle tohoto zákona.

(2) Do práva autorského neoprávněně zasahuje také ten, kdo vyrábí, dováží, přijímá, rozšiřuje, prodává, pronajímá, propaguje prodej nebo pronájem nebo drží k obchodnímu účelu zařízení, výrobky nebo součástky nebo poskytuje služby, které

a) jsou za účelem obcházení účinných technických prostředků nabízeny, propagovány nebo uváděny na trh,

b) mají vedle obcházení účinných technických prostředků jen omezený obchodně významný účel nebo jiné užití, nebo

c) jsou určeny, vyráběny, upravovány nebo prováděny především s cílem umožnit nebo usnadnit obcházení účinných technických prostředků.

(3) Účinnými technickými prostředky podle tohoto zákona se rozumí jakákoli technologie, zařízení nebo součástka, která je při své obvyklé funkci určena k tomu, aby zabraňovala nebo omezovala takové úkony ve vztahu k dílům, ke kterým autor neudělil oprávnění, jestliže užití díla může autor kontrolovat uplatněním kontroly přístupu nebo ochranného procesu jako je šifrování, kódování nebo jiná úprava díla nebo uplatněním kontrolního mechanismu rozmnožování.

(4) Právní ochranou podle odstavce 1 nejsou dotčena ustanovení § 30a, § 31 odst. 1 písm. b), § 34 písm. a), § 37 odst. 1 písm. a) a b), § 38, § 38a odst. 2 a § 38e v rozsahu nezbytném k využití výjimky. Autor, který pro své dílo použil technické prostředky podle odstavce 3, je povinen zpřístupnit své dílo oprávněným uživatelům v rozsahu nezbytném

ke splnění účelu uvedeného užití díla. Autor může zpřístupnit své dílo, pro které použil technické prostředky podle odstavce 3, i v případě zhotovení záznamu svého díla pro osobní potřebu podle § 30; to nebrání autorovi, aby přijal odpovídající opatření týkající se počtu takových rozmnoženin.

(5) Ustanovení odstavce 4 se nevztahuje na dílo, které bylo autorem či s jeho souhlasem zpřístupněno veřejnosti způsobem podle § 18 odst. 2.

(6) Technické prostředky ke splnění povinností podle odstavce 4 používané autorem dobrovolně nebo na základě dohod požívají ochrany podle odstavců 1 až 3.“ [6]

Závěr z tohoto paragrafu je jednoznačný, právo na vytvoření kopie z chráněného disku zaniká [23]. Tohle až donedávna neplatilo, omezení je platné od 22. května 2006, kdy vydal parlament sbírku zákonů č. 216/2006 Sb., který autorský zákon novelizuje.

11.3 Tresty hrozící za porušení autorského práva

1. ledna 2010 začal platit úplně nový Trestní zákoník uvedený jako zákon č. 40/2009 Sb. V § 270 nazvaném Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi se píše:

„(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo

c) dopustí-li se takového činu ve značném rozsahu.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.“ [7]

V porovnání s § 152 z dnes už neplatného zákona č. 140/1961 Sb. se kromě možností propadnutím věci (např. počítače a DVD nosičů), peněžitého trestu zvyšuje pouze maximální možná hranice odnětí svobody z 5 [24] na 8 let.

V posledních letech se množí především případy, kdy propuštěný zaměstnanec udá svého bývalého zaměstnavatele, že využívá nelegální software. Proto by si správci sítí měli dávat velký pozor, aby nemuseli strávit nějaký ten rok jako trestanci.

11.4 Zákon o ochraně spotřebitele

Zákon 634/1992 Sb. o ochraně spotřebitele prošel od roku 1992 celkem 23 úpravami, poslední novelizace byla provedena zákonem č. 36/2008 Sb. s účinností od 17. ledna 2008. Zákon o ochraně spotřebitele má jako ve všech oblastech prodeje své místo i při prodeji audiovizuálních děl. [7] V zákonu se v § 9 píše:

„(1) Prodávající je povinen řádně informovat spotřebitele o vlastnostech prodávaných výrobků nebo charakteru poskytovaných služeb, o způsobu použití a údržby výrobku a o nebezpečí, které vyplývá z jeho nesprávného použití nebo údržby, jakož i o riziku souvisejícím s poskytovanou službou. Jestliže je to potřebné s ohledem na povahu výrobku, způsob a dobu jeho užívání, je prodávající povinen zajistit, aby tyto informace byly obsaženy v přiloženém písemném návodu a aby byly srozumitelné.

(2) Povinností uvedených v odstavci 1 se nemůže prodávající zprostit poukazem na skutečnost, že mu potřebné nebo správné informace neposkytl výrobce, dovozce nebo dodavatel. Tyto povinnosti se však nevztahují na případy, kdy se jedná o zřejmé nebo obecně známé skutečnosti.“ [7]

Z toho úryvku vyplývá, že prodejce musí kupujícího informovat o tom, zda je na CD / DVD použitá ochrana proti kopírování, popřípadě jaká z toho vyplývají omezení (např. audio CD není možno přehrávat na počítači). [7]

ZÁVĚR

Cílem této bakalářské práce bylo systematicky a přehledně seznámit čtenáře s výhodami a nevýhodami ochran proti kopírování na CD, DVD a Blu-ray discích. Aby bylo možno snáze pochopit některé ochrany, je součásti práce i historický vývoj optických médií, jejich technické parametry a vlastnosti. Rozmanitost ochran proti kopírování softwarových produktů je natolik široká, že by se pouze o této oblasti dala napsat celá práce. Společnosti, které se zabývají vývojem a implementací takovýchto ochranných technologií, by ale musely poskytnout detaily, které si, z pochopitelných důvodů, pečlivě chrání. Kromě ochran programů a her byly představeny i některé ochrany proti kopírování používané u hudebních CD, filmových DVD a Blu-ray disků. Informace obsažené v této práci jsou shromážděny především z renomovaných serverů nebo přímo ze stránek výrobce dané technologie.

V druhé části práce byla nastíněna možnost obcházení ochranných prostředků. Účelem nebylo propagovat tyto programy ani nabádat k prolamování ochran, ale poukázat na soupeření mezi výrobci chráněných disků a výrobci softwarových produktů na detekci a deaktivaci ochrany, což vede k vytvoření kopie disku. Další kapitola byla věnována možnosti výroby vlastního chráněného média na běžné vypalovací mechanice. Úspěšně byla otestována ochrana heslem i ochrana digitálním podpisem. Řešení je ideální především v případě, že chceme zabezpečit a vypálit data, jejichž zneužití by mohlo mít nedozírný vliv na nás samotné nebo organizaci, která s takovými citlivými daty pracuje. Aby byla problematika kopírování a obcházení technických prostředků ochrany práv kompletní, je poslední kapitola věnována legislativě.

Dle mého názoru je určitým způsobem boj mezi vydavatelstvími se softwarovými a audiovizuálními piráty pochopitelný. Následky však často nesou i slušní zákazníci, kteří si legální cestou zakoupí originální disk s ochranou proti kopírování a pro případ nechtěného poškození si nemůžou vytvořit ani záložní kopii pro vlastní potřebu. Nelze předpokládat, že od používání těchto kopírovacích ochran se jednou pro vždy upustí. Teoreticky by se tak dalo učinit, ale musel by se nejdříve změnit nejen postoj společnosti k originálním médiím a neposkytovat je dalším osobám, ale také postoj distributorů a vydavatelství k ceně, za kterou jsou ochotni film, software nebo hudbu prodávat. Těžko si ale dokážu představit, že si tyto subjekty zvyknou na mnohem nižší tržby za prodaný kus nosiče. Ceny se postupně opravdu snižují, ale společnost vytváří kopie disků již automaticky nebo stahuje obrazy dat

pomocí Internetu. Proto si myslím, že situace bude spíše opačná a budou se zdokonalovat jak výrobci ochran proti kopírování, tak i vývojáři softwarových a hardwarových technologií.

ZÁVĚR V ANGLIČTINĚ

The goal of this bachelor project was to systematically and clearly inform the reader about the advantages and disadvantages of copy protections emplaced on CDs, DVDs and Blu-ray discs to prevent unauthorized duplication. To help the reader better understand the various copy protections, part of the project focused on the historical development of optical media, their properties and technical parameters. The variety of protections against copying of software products is so vast, that it would be possible to focus the project entirely on this one area, and thus companies which research, create, and then implement such copy protection technologies would have to provide details, which, understandably, keep such information secret. Apart from copy protection on programs and games, the project also presents some of the protections used on audio CDs, film DVDs and Blu-ray discs. Information contained within this work was gathered foremost from successful servers or directly from websites created by the developers of the relevant technologies.

The second part of the work mentions methods used to bypass various copy protections. The aim, however, was not to promote such programs nor assist in breaking through such technologies, but to demonstrate the competition between creators of protected discs and developers of software products which detect or bypass such safeguards, leading to copies of the disc and its contents. The next chapter was dedicated to options for the creation of one's own protected media using standard burning hardware. Password protection and protection via digital signature was tested successfully. This solution is ideal in the case that we need to protect and burn data which, if misused, would have unforseen detrimental consequences to us personally, or to organizations which work with such sensitive data. To ensure that the problems encountered when dealing with the illegal copying and bypassing of technical aspects within copy protection technologies are complete, the final chapter focuses on legislature.

To a certain degree, the fight between publishers and software or audio/visual pirates is understandable, in my opinion. Unfortunately, the consequences often affect even honest customers which, by legal means, acquire an original disc with some form of copy protection, and in the case they should accidentally damage their disc, cannot create a backup copy of the disc for personal use. It is reasonable to assume, however, that the use of copy protection technologies will not decline nor cease. Theoretically it is possible to reach such an actuality, but first the stance towards orginial media would have to change in

both the general public, which would have to respect copyright and not allow or resort to piracy, as well as the stance of distributors and publishers, which would need to concede to a price which is considered reasonable for the film, software, or music they are attempting to sell. I find it hard to believe, however, that the afore-mentioned subjects would acclimatize to a more modest yield per capita. Prices are, in fact, systematically lowering, yet the general public replicate discs frequently, or download data images via the Internet. Therefore, it is my assumption that the situation will most likely turn in the opposite direction, where designers of copy protection technologies will further perfect their products, as will developers of software and hardware technologies.

SEZNAM POUŽITÉ LITERATURY

[1] TAYLOR, Jim, JOHNSON, Mark R., CRAWFORD, Charles G. Velký průvodce DVD : Jedinečný zdroj všech dostupných informací o DVD na profesionální úrovni. 1. vyd. Praha : Grada Publishing, 2007. 552 s. ISBN 978-80-247-1721-0.

[2] Deep in IT : Informace ze světa počítačů o hardware, software, Internetu atd. [online]. 2010 [cit. 2010-01-28]. Dostupný z WWW: <http://www.diit.cz/>.

[3] BROŽA, Petr. Vypalujeme CD pomocí programu Nero. Praha : Computer Press, 2003. 113 s. ISBN 80-7226-775-2.

[4] BRÜGMANN, Ulrich. Gecheckt – Geheckt : Spiele kopieren. [United States of America] : Lulu Enterprises, 2007. 94 s. ISBN 978-3-00-022964-0.

[5] HAVELKA, Jiří. Velká kniha vypalování CD a DVD. 2. aktualiz. vyd. Brno : CP Books, 2005. 470 s. ISBN 80-251-0629-2.

[6] Autorský zákon [online]. 2009 [cit. 2010-01-28]. Dostupný z WWW: <http://cs.wikisource.org/wiki/Autorský_zákon>.

[7] Businesscenter.cz [online]. 2010 [cit. 2010-04-02]. Zákony a právní normy. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/>.

[8] TAYLOR, Jim, et al. Blu-ray Disc Demystified. 1st edition. [United States of America] : McGraw-Hill, 2009. 432 s. ISBN 978-0-07-159092-1.

[9] DVD-R.CZ [online]. 2008 [cit. 2010-04-03]. CD, DVD a Blu-Ray encyklopedie. Dostupné z WWW: <http://www.dvd-r.cz/cz/cd-dvd-blu-ray-encyklopedie.php>.

[10] KLABAZŇA, Petr. SVĚT HARDWARE [online]. 13.7.2001 [cit. 2010-04-03]. Ring PROTECH - nová (prý neporazitelná) ochrana proti pirátskému kopírování CD. Dostupné z WWW: <http://www.svethardware.cz/disc_doc-N73CF02B8539EA5F5C1256A88004AA3FE.html>.

[11] CDRinfo [online]. 2010 [cit. 2010-04-03]. The Hardware Authority . Dostupné z WWW: <http://www.cdrinfo.com/>.

[12] CD Media Word [online]. 2007 [cit. 2010-04-03]. SafeDisc Advanced. Dostupné z WWW: <http://www.cdmediaworld.com/hardware/cdrom/files/sdadv_datasheet .pdf>.

[13] Link Data Security [online]. 2010 [cit. 2010-04-03]. Piracy Protection for CDs, DVDs and the web. Dostupné z WWW: <http://linkdata.dk/>.

[14] LaserLock [online]. 2009 [cit. 2010-04-03]. Copy Protection Architects. Dostupné z WWW: <http://www.laserlock.com>.

[15] Array Data [online]. 2005 [cit. 2010-04-03]. OCHRANA KOPÍROVÁNÍ DVD PRO ON-DEMAND DISC PUBLISHING. Dostupné z WWW: <http://www.array.cz/rimage/pdf/DVDCopyProtect.pdf>.

[16] DCS Copy Protection Ltd [online]. 2010 [cit. 2010-04-03]. Latest News. Dostupné z WWW: <http://www.dwightcav.com/>.

[17] PC World [online]. 27. 04. 2009 [cit. 2010-04-03]. GE vyvinula materiál pro optický disk schopný pojmout 500 GB dat. Dostupné z WWW: <http://pcworld.cz/novinky/ge-vyvinula-material-pro-opticky-disk-schopny-pojmout-500-gb-dat-7167>.

[18] Physorg.com [online]. 30. 9. 2009 [cit. 2010-04-03]. GE Shows Off 1TB DVD-Sized Disks at the Emerging Tech Conference. Dostupné z WWW: <http://www.physorg.com/news173550252.html>.

[19] StarForce [online]. 2010 [cit. 2010-04-19]. FrontLine Disc. Dostupné z WWW: <http://www.star-force.com/solutions/products/fl_disc/>.

[20] SlySoft.com [online]. 2010 [cit. 2010-04-19]. SlySoft Products. Dostupné z WWW: <http://www.slysoft.com>.

[21] SecurDisc [online]. 2010 [cit. 2010-04-19]. SecurDisc - Discover a new dimension in data protection. Dostupné z WWW: <http://www.securdisc.net>.

[22] LOHNISKÝ, Jakub. 222 tipů a triků pro vypalování CD. Praha : Computer Press, 2002. 94 s. ISBN 80-7226-634-9.

[23] Česká protipirátská unie [online]. 2010 [cit. 2010-04-19]. F.A.Q. - Často kladené otázky. Dostupné z WWW: <http://www.cpufilm.cz/faq.html>.

[24] CMAJDÁLKA, Lukáš. Metodika vyšetřování softwarového pirátství. 2008. 76 s. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A/D převodník	Obvod pro převod analogového signálu na digitální
AACS	Advanced Access Content System
AES	Advanced Encryption Standard
APS	Analog Protection System
BCA	Burst Cutting Area
BD	Blu-ray disk
BD-ROM	Blu-ray disky určené pouze ke čtení
CD	Kompaktní disk
CD-DA	Audio CD
CD-Extra	Varianta Audio CD umožňující ukládat mimo hudbu i další soubory
CD-R	Zapisovatelné CD
CD-ROM	Rozšířená varianta Audio CD pro ukládání počítačových dat
CD-RW	Přepisovatelné CD
CGMS	Copy Generation Management System
CPPM	Content Protection for Prerecorded Media
CPRM	Content Protection for Recorded Media
CSS	Content Scrambling System
DTCP	Digital Transmission Content Protection
DVD	Digital Versatile Disc
DVD-Audio	Pouze zvuková varianta DVD
DVD-R	Zapisovatelné DVD
DVD-ROM	Základní formát pro DVD
DVD-RW	Přepisovatelné DVD
DVD-Video	Standard pro ukládání zvuku a videa na DVD-ROM

GB	Giga bajt
HDCP	High-bandwidth Digital Content Protection
HVD	Holographic Versatile Disc
kB	Kilo bajt
MB	Mega bajt
TB	Tera bajt
TOC	Table of Contens
VTS	Video Title Set
WMP	Windows Media Player

SEZNAM OBRÁZKŮ

SEZNAM TABULEK