UNIVERSITÀ DEGLI STUDI DI SALERNO

FACOLTÀ DI SCIENZE NATURALI FISICHE E MATEMATICHE

Corso di laurea in Informatica

Tesina di Sicurezza su Reti 2

Digital Rights Management

Professore
Alfredo De Santis

Studente
Costante Luca
Matr. 0521000838

Anno Accademico 2008/2009

INDICE

INDICE DELLE FIGURE

INTRODUZIONE

Con Digital Rights Management (DRM) [1], il cui significato letterale è "gestione dei diritti digitali", si intendono i sistemi tecnologici mediante i quali i titolari di diritto d'autore (e dei cosiddetti diritti connessi) possono esercitare ed amministrare tali diritti nell'ambiente digitale, grazie alla possibilità di rendere protette, identificabili e tracciabili le opere di cui sono autori.

Tramite i DRM, i file audio o video vengono codificati e criptati in modo da garantire una più difficile diffusione, impedimenti all'utenza e consentirne un utilizzo:

- limitato (ad esempio solo per determinati periodi di tempo o per determinate destinazioni d'uso);
- predefinito nella licenza d'accesso fornita (separatamente) agli utenti finali.

Figura 1 DRM

I file così prodotti portano con sé le diciture di copyright, e possono essere arricchiti con altre informazioni, come immagini, biografia degli autori, collegamenti, ecc. L'accesso ai contenuti da parte degli utenti finali avviene secondo procedure di profilazione e autenticazione che permettono di distribuire i file richiesti nelle modalità previste dalla licenza sottoscritta dall'utente.

L'attivazione di un codice seriale, che corrisponde al costo di licenza, era una modalità di difesa del diritto d'autore, più facile da violare rispetto ai sistemi di DRM. La validazione del codice può avvenire direttamente sul computer oppure con un collegamento ad Internet al sito del produttore; per molti programmi esistono dei keygen, categoria di programmi che generano un seriale valido per sbloccare altri software. Dall'esame di molti seriali di un dato prodotto, si riusciva interpolare e ricostruire l'algoritmo di generazione dei codici, tenuto segreto dal produttore.

1.1. Storia

Con l'avvento delle tecnologie digitali, copiare un file multimediale (audio o video) è diventato semplice e non comporta, a differenza dei supporti analogici, una diminuzione della qualità.

Grazie alla diffusione di strumenti digitali per l'accesso a contenuti multimediali, quali personal computer, mp3 player, telefonini di nuova generazione, lettori di divx e alla diffusione dell'accesso a Internet a banda larga e delle reti peer to peer, l'accesso e la distribuzione in tutto il mondo di contenuti multimediali è alla portata di ogni singolo utente, creando nuovi scenari capaci di modificare il consolidato sistema autore-distributore-cliente, a danno del distributore e talvolta dell'autore.

Lo studio di soluzioni DRM nasce dal tentativo di poter gestire il controllo sugli aspetti legati alla distribuzione e all'utilizzo. Le prime forme di DRM, avute negli anni ’70, venivano applicate essenzialmente sui contenuti artistici e letterali. Il boom dell’utilizzo dell’uso dei DRM si è avuto con la diffusione dell’audio e del video digitale. Il primo vero esempio di DRM digitale si è avuto nel 1996 con il sistema CSS (Content

Scrambling System). Il CSS è un semplice algoritmo di cifratura utilizzato dalla major cinematografiche per la diffusione dei propri film con l'inclusione di restrizioni di riproduzione e copia. La figura sotto mostra gli anni in cui le tecniche che sono state studiate sono state realizzate.

Anno	Nome
Anni '70	Applicazioni su contenuti artistici e letterali
1996	Content scrambling system (CSS)
1996	DVD Region Code
1998	Digital Transmission Content Protection (DTCP)
1999	Windows Media DRM
2001	Content Protection for Recordable Media (CPRM)
2003	FairPlay
2005	Extended Copy Protection (XCP)
2005	L'Advanced Access Content System (AACS)
2008	BD+

Figura 2 Tabella Storia protezioni

1.2. Dominio di applicazione

1.2.1. Attivazione del software

Microsoft è stata la prima azienda a implementare un meccanismo di attivazione del software nei suoi prodotti nel 1995 con il rilascio di *Windows 95*.

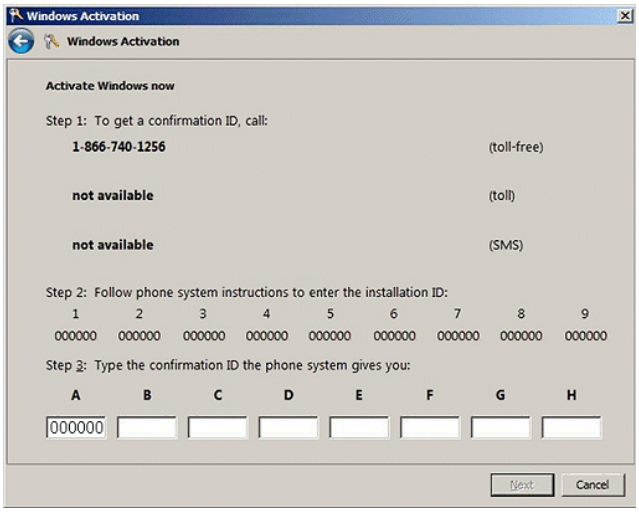

Figura 3 Esempio di Attivazione del Software

In seguito la tecnologia di attivazione è stata implementata in Windows XP e Office XP. In ambo i casi l'utente, acquistando il software originale, riceve un codice alfanumerico di 25 caratteri, la cui validità viene inizialmente verificata dal software stesso tramite un algoritmo di hashing. Entro un periodo stabilito (30 giorni) l'utente deve eseguire una verifica online o telefonica comunicando un codice numerico generato in base alla product key e alla configurazione hardware del PC su cui il software è installato. Se la verifica ha successo, il server (o l'operatore) risponde con un codice di conferma riconosciuto dal sistema, che sblocca tutte le sue funzionalità.

La tecnologia di attivazione è oggi adottata da tantissimi produttori di software, ma nella maggior parte dei casi può essere aggirata tramite reverse engineering.

1.2.2. Audio e Film

Uno dei primi sistemi DRM conosciuti è il Content Scrambling System (CSS), ideato dal DVD Forum per i film in DVD. Tale sistema prevede la cifratura dei supporti con una chiave segreta rilasciata ai produttori di hardware e software di lettura a patto di accettare specifiche condizioni di licenza (e pagare una quota), tra cui il divieto, ad

esempio, di fornire audio digitale ad alta qualità; quindi, i DVD video con questa particolare tecnologia non potranno essere masterizzati e/o copiati. Per copiarli o masterizzarli si deve disporre di programmi di decodifica CSS (come Any DVD o DVD Region+CSS Free); questi Programmi di decodifica CSS si possono usare solo negli Stati in cui è permesso il loro uso.

Anche per i file audio regolarmente acquistati nei negozi di musica digitale in Internet vari schemi di DRM sono stati direttamente integrati nei file per costringere l'utente ad una serie di limitazioni, come ad esempio il limite del numero di dispositivi o tipi di dispositivi sui quali quei file possono essere riprodotti.

1.2.3. Internet music shop

Numerosi negozi online di musica fanno uso dei DRM per ridurre l'uso del file musicale scaricato. Esistono diversi negozi online che vendono musica oppure file audio-visivi e più conosciuti sono:

- iTunes Store[6], della Apple Inc., permette ai propri clienti di acquistare online i brani a soli $0.99 US. Ogni brano acquistato usa il sistema DRM della Apple chiamato FairPlay. A causa della rottura da parte di un hacker di questo sistema di protezione, il 6 Gennaio 2009 la Apple ha annunciato che i brani che vengono venduti on line su iTunes sono senza DRM.
- Napster music store: offre ai proprio clienti un approccio diverso rispetto a quello offerto da iTunes. Infatti il DRM non è previsto per ogni singola traccia ma per ogni singolo utente. Ogni utente può scaricare o ascoltare in streaming un numero illimitato di musica codificata con Windows Media Audio (WMA). Quando il periodo della sottoscrizione termina, tutti i brani musicali scaricati non possono essere più riprodotti fino a quando l'utente non decide di rinnovarla. Napster inoltre permette ad un utente registrato di poter utilizzare i brani scaricati su un dispositivo portabile per un costo aggiuntivo di $5 al mese.

Infine, con un costo aggiuntivo di $0.99 per brano, Napster permette di masterizzare i brani su un CD.

- Sony mette a disposizione dei proprio clienti un servizio online di download di musica chiamato "Connect" dove ogni brano usa la tecnologia DRM OpenMG la quale permette l'utilizzo dei brani esclusivamente su un pc che utilizza Windows o che abbia un hardware (PSP inclusa).

Alcuni negozi online di musica quali eMusic, Dogmazic, Amazon, e Beatport non fanno uso dei DRM per incoraggiare gli utenti ad evitare la condivisione della musica.

1.2.4. Videogiochi

I produttori di videogames utilizzano i DRM per limitare il numero di PC su cui il gioco può essere installato (in genere da 3 a 5 installazioni). Questa tecnica è stata introdotta proprio per evitare lo scambio di giochi tra gli utenti.

1.2.5. EBook

Molti produttori di eBook (electronic Book) usano una implementazione simile di DRM per limitare il numero di computer sui quali l'eBook può essere visualizzato, copiato, letto, stampato o condiviso.

I principali programmi che fanno uso dei DRM per gli eBook sono Adobe Acrobat e Microsoft Reader. Con Microsoft Reader, gli eBook acquistati venivano protetti dalla copia non autorizzata mediante la connessione, attraverso la rete Internet, ad un server cui venivano fornite informazioni che identificavano il dispositivo e il file. Se l'utente aveva realmente acquistato il prodotto, la lettura poteva iniziare.

In generale, una volta che l'utente ha aperto il PDF, può visionare i diritti e svolgere solo le operazioni per cui ha i permessi.

1.3. Opinioni contrarie

Molte organizzazioni, artisti individuali, informatici si sono opposti ai DRM. Le pesanti conseguenze di tali sistemi anche per gli utenti di contenuti legittimamente acquistati viene motivata da una forte campagna internazionale contro lo scambio (definita pirateria informatica dalle major) di tali contenuti, condotta dalle case discografiche e cinematografiche, che ha sollevato forti critiche. Tale campagna è osteggiata anche dagli stessi autori. In Canada, ad esempio, è stata fondata da artisti quali Avril Lavigne, Barenaked Ladies e Sarah McLachlan la Canadian Music Creators' Coalition (CMCC) [7], che si oppone con forza ai DRM, il cui manifesto è: "Gli artisti non vogliono promuovere cause legali contro i propri fan e le case discografiche hanno intentato ai nostri fan contro la nostra volontà, e le leggi che consentono tali cause non possono essere giustificate in nostro nome"; il manifesto prosegue facendo capire che i DRM non sono negli interessi dei consumatori, e implicitamente neanche negli interessi degli artisti, e chiedono al governo di considerare modi diversi per la promozione degli artisti.

Figura 4 Logo CMCA

Già negli anni ottanta, con la produzione di nuovi software, si cominciava a sperimentare queste nuove tecnologie per la protezione dei contenuti, ma solo con la diffusione in massa delle opere audio e audiovisive, le case di produzione e distribuzione iniziarono a implementare sistemi DRM sui propri supporti.

CAPITOLO 2: CD & DVD

2.1. CD

Il compact disc, in sigla CD, è una tipologia di disco ottico utilizzata in vari ambiti per la memorizzazione di informazioni in formato digitale.

Il compact disc è composto da un disco di policarbonato trasparente, generalmente di 12 centimetri di diametro, che racchiude al suo interno un sottile foglio di materiale metallico sul quale sono memorizzate le informazioni come successioni di "buchi" e "terre" (in inglese "pits" e "lands") successivamente letti per mezzo di un laser (per questo motivo sono detti anche dischi ottici).

Figura 5 Compact Disc

I CD hanno una struttura paragonabile a quella dei normali dischi musicali: i dati sono ordinati lungo un'unica traccia a forma di spirale, un'organizzazione quindi molto diversa da quella dei dischi magnetici (hard disk e floppy disk). La spirale parte al centro (contrariamente ai dischi in vinile) e procede verso l'esterno, permettendo così di avere CD più piccoli dello standard (per esempio i mini-CD o i CD a forma di carta di credito).

Quando i CD furono inventati, le macchine duplicatrici erano costosissime e 650 MB sembravano un'enormità. Oggi tali macchine sono estremamente a buon mercato, e chiunque può creare una copia perfetta di un CD (audio, dati, video), spendendo meno di 1 euro.

2.2. Le protezioni dei CD

2.2.1. LaserLock

Realizzata da LaserLock International [2], utilizza una traccia impressa sul CD durante la procedura di masterizzazione LaserLock chiamata appunto LaserLoching. Durante questa fase che viene effettuata dalle casi produttrici (solitamente di videogiochi), vengono inseriti dei file danneggiati in una cartella nascosta (chiamata LaserLock) i quali non permettono la masterizzazione poiché inducono ad errori. Per superare questa protezione, basta copiare il contenuto del disco esclusa la cartella nascosta sul PC e successivamente effettuare la masterizzazione.

2.2.2. SecuROM

SecuROM [4] è uno dei metodi di protezione più conosciuti, sviluppato dalla Sony e applicato maggiormente ai videogames.

Il supporto viene masterizzato da una macchina particolare la quale inserisce dei file che contengono informazioni sulla struttura dati del CD. Questi file risultano incopiabili in quanto registrabili soltanto da questa particolare macchina. La protezione, può essere individuata grazie alla presenza, sulla confezione del CD, dell'immagine SecuROM (vedere figura sotto).

Figura 6 SecureROM

2.2.3. TOC fasullo

Questa protezione, consiste nel far apparire il cd di dimensione maggiore di un 1 Gb (1024 Mb), mentre, come sappiamo tutti, un cd non può contenere più di 700 Mb. Ciò è possibile scrivendo una falsa tabella dei contenuti (TOC) e nel momento in cui si avvia il programma per masterizzare, si riceve un messaggio di errore ancor prima di iniziare la masterizzazione.

2.2.4. CD-Cops

Questa protezione dalla copia funziona come segue: CD-Cops [5] legge il CD e misura la velocità di lettura. Questo valore, rappresentato da un numero (il codice), che viene inserito nel disco e costituisce la chiave del CD (detto anche "CD key"). Se il CD inserito ha una differente velocità di lettura (confrontata con il numero memorizzato), il CD non funzionerà dato che la chiave è differente. Viene utilizzato principalmente per proteggere i videogiochi e durante la fase di installazione, l'eseguibile provvede a controllare la validità del CD key e nel caso in cui quello memorizzato non corrisponde a quello calcolato, la procedura di installazione verrà interrotta.

2.2.5. DiscGuard

DiscGuard è una tecnologia anti-pirata per i supporti ottici, che funziona inserendo una "firma" non riproducibile nè dai dischi contraffatti nè attraverso la comune

masterizzazione. In questo modo, un pirata che cercherà di duplicare un disco DiscGuard riuscirà solamente a copiarne il contenuto, ma non la firma inserita.

2.3. DVD

Il DVD, acronimo di Digital Versatile Disc (in italiano Disco Versatile Digitale, originariamente Digital Video Disc, Disco Video Digitale) è un supporto di memorizzazione di tipo ottico.

Il DVD è il prodotto della cooperazione di alcune fra le maggiori aziende nel campo della ricerca e dell'elettronica di consumo: il cosiddetto DVD forum [10], ovvero l'istituzione che si è incaricata di redigere le specifiche del nuovo supporto, era infatti formata da Philips, Sony, Matsushita, Hitachi, Warner, Toshiba, JVC, Thomson e Pioneer. L'intento era quello di creare un formato di immagazzinamento di grandi quantità di video digitali che fosse accettato senza riserve da tutti i maggiori produttori, evitando quindi tutti i problemi di incertezza del mercato dovuti alla concorrenza fra formati che si erano presentati al tempo dell'introduzione delle videocassette per uso domestico.

Il DVD forum individua 3 principali campi d'applicazione per il DVD:

1. il DVD-Video, destinato a contenere film, in sostituzione della videocassetta;
2. il DVD-Audio, pensato per sostituire il CD Audio grazie a una maggiore fedeltà e capacità;
3. il DVD-ROM, destinato a sostituire il CD-ROM.

Sia nel DVD-Video che nel DVD-Audio sono previsti sistemi di protezione in grado di disincentivare la duplicazione dei contenuti.

In un secondo momento, lo stesso DVD Forum introdusse gli standard per i formati registrabili del DVD. Formalizzato nel corso del 1999, il formato DVD-R è lo standard ufficiale per i DVD Registrabili. Esso si suddivide nei formati "DVD-R for authoring" e "DVD-R for general use". I primi sono destinati alla creazione di copie di video protette

da diritto d'autore, necessitano di uno speciale masterizzatore e sono in grado di implementare i sistemi di protezione dalla duplicazione. La differenza fondamentale tra i due formati risiede nella diversa lunghezza d'onda del laser: 635 nm per il DVD-R(A) e 650 nm per il DVD-R(G). I secondi sono in grado di contenere qualunque tipo di materiale, ma non sono compatibili con i sistemi di protezione utilizzati nei DVD-Video.

Le dimensioni dei DVD di produzione industriale sono di quattro tipi:

- ✓ DVD-5: 4,7 GB Lato unico e singolo strato
- ✓ DVD-9: 8,5 GB Double layer Lato unico e doppio strato
- ✓ DVD-10: 9,4 GB Due lati e singolo strato
- ✓ DVD-18: 17 GB Due lati e doppio strato

I DVD "double layer" permettono una doppia incisione nello stesso lato. La capacità del supporto non raddoppia esattamente, perché una parte di memoria è dedicata alla creazione di un indice e al controllo della distribuzione dei dati.

Per il double layer occorre un particolare masterizzatore con tale funzionalità. Per il double side è sufficiente avere un supporto a doppio strato, che viene inciso con i comuni masterizzatori, semplicemente girando il disco.

Il file system del DVD è una variante ridotta dell'UDF (Universal Disc Format), chiamata MicroUDF.

La struttura dei DVD-Video, cioè il modo in cui i file sono memorizzati ed organizzati all'interno del supporto di memorizzazione, è standard; questa organizzazione serve a fare in modo che tutti i riproduttori siano in grado di localizzare senza problemi i dati.

All'interno della radice vi sono due directory, chiamate AUDIO_TS e VIDEO_TS. Come i nomi suggeriscono, queste due directory sono deputate a contenere rispettivamente gli elementi dei DVD-Audio e dei DVD-Video.

All'interno di VIDEO_TS vi sono tre tipi di file, identificati da tre differenti estensioni:

- .IFO: contiene le informazioni sulla dislocazione di audio, video e sottotitoli, sulla suddivisione in capitoli del film e su ogni altro contenuto; è il descrittore della struttura del DVD-Video;
- .VOB: VOB sta per Video OBject; è il contenuto multimediale vero e proprio, cioè è un file è in cui sono memorizzati l'audio e il video in forma multiplexata, cioè miscelata;
- .BUP: è un backup del file .IFO.

La figura 7 mostra il contenuto di un disco DVD-Video.

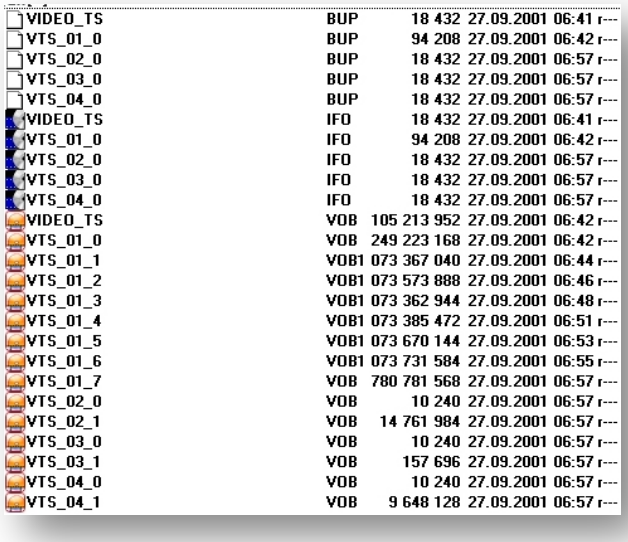

Figura 7 Struttura del file System di un DVD Video

Siccome le specifiche stabiliscono che un file .VOB abbia una grandezza massima di 1 Gigabyte (1.073.739.776 bytes), un tipico film di 90-100', che occupa, in compressione MPEG-2, dai 4 ai 6 Gigabyte, verrà suddiviso in più file .VOB.

Oltre ad avere specifiche estensioni, i file presenti nella directory VIDEO_TS sono anche caratterizzati da una specifica nomenclatura. I nomi dei file possono iniziare per:

- VIDEO_TS

- VTS_

dove TS è l'acronimo di TitleSet.

I file che cominciano per VIDEO_TS sono i primi ad essere letti e contengono le informazioni ed i contenuti riprodotti automaticamente quando il supporto viene inserito nel lettore (p.es. le informazioni di copyright e il menu principale del DVD). Gli altri file, che iniziano per VTS_, racchiudono tutte le altre informazioni e contenuti. Gli archivi .IFO contengono i riferimenti ai .VOB da caricare; un singolo file .IFO può gestire al massimo 10 file .VOB.

2.4. Le protezioni dei DVD Video

La storia del DVD-Video è strettamente interrelata a quella dei sistemi di protezione dei contenuti, che i produttori hanno voluto fossero presenti in questo supporto fin dalle primissime versioni. L'elevato livello qualitativo dello standard MPEG-2, che rendeva possibile fruire in home video di una qualità di gran lunga superiore a quella del VHS, intimoriva moltissimo le major cinematografiche, la cui pretesa, fin dal 1994, era che sul nuovo supporto venissero memorizzate soltanto copie a bassa risoluzione dei video originali. Solo nel 1996, quando fu introdotta una serie di misure, anche a livello di normativa legale, volte a limitare il fenomeno della pirateria audiovisiva, i produttori acconsentirono all'uso del DVD per le applicazioni Video.

Anzitutto, le case cinematografiche avevano preteso la suddivisione del globo in sei macro aree principali, che sarebbero servite ad impedire lo scambio di DVD fra una nazione e l'altra, a causa delle incompatibilità dei rispettivi lettori (un lettore con codice per la zona 6 non è in grado di leggere un DVD contrassegnato per la zona 1).

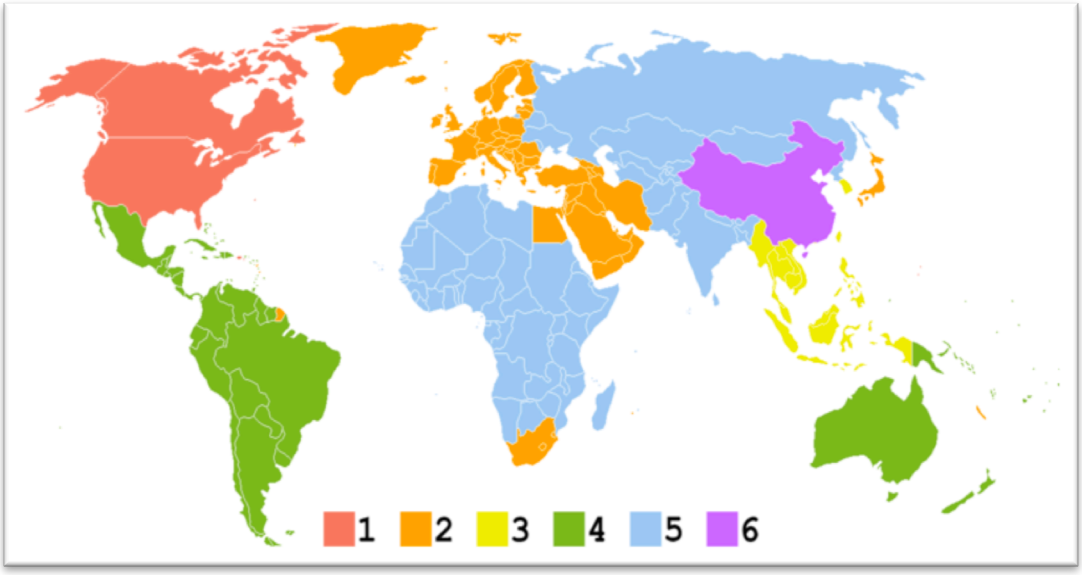

Figura 8 Le zone dei DVD

Inoltre furono implementati altri due sistemi di protezione: un primo sistema era deputato ad impedire la copia analogica (il Macrovision) mentre il secondo era volto ad impedire la copia digitale, cioè il "copia e incolla", via sistema operativo, dei files contenenti il video. Quest'ultimo tipo di protezione, chiamato Content Scrambling System (acronimo: CSS), veniva considerato, dai produttori, come la garanzia definitiva contro la riproduzione illegale.

2.4.1. Analog Protection System (Macrovision)

La protezione Macrovision è stato uno dei primi tipi di protezione (introdotta nel 1999), fu implementato originariamente per impedire la duplicazione delle videocassette VHS. Non solo i videoregistratori e lettori DVD da tavolo sono dotati di questo circuito ma anche le normali schede video dotate di TV-Out, che hanno sull'uscita video la protezione. I film copiati dai DVD sulle VHS, che sono stati protetti con APS, diventano incomprensibile e inguardabili. Il suo scopo principale era quello di impedire la copia sull'uscita analogica.

APS è un tipo di protezione hardware e consistente nell'invio di un picco di tensione sull'uscita video analogico di un qualunque riproduttore dotato del circuito apposito; la tensione viene inviata una volta ogni tot secondi, come codificato nel DVD-Video, che deve essere specificamente stampato in modo da prevedere questo tipo di protezione. Il picco di tensione sull'uscita del lettore comporta il fatto che un eventuale altro lettore, che prenda in ingresso questo flusso, visualizzerà una serie di artefatti, o di fotogrammi illeggibili, ogni tot fotogrammi integri.

Il segnale distorto manda fuori fase la gestione automatica del sistema di sincronismo verticale del lettore che sta prendendo in input lo stream, causando memorizzazione di fotogrammi caratterizzati da forti variazioni di luminosità. Inoltre, la distorsione comporta anche cambi di informazioni colorbust. Il risultato finale sarà un video inguardabile, perché pieno di quadretti colorati, bagliori e spezzoni indecifrabili.

2.4.2. Content Scrambling System (CSS)

In supporto DVD, il film è costituito da file VOB, criptati dal sistema CSS [15]. Una copia diretta dei file dal DVD ad un altro supporto (ad esempio, un hard disk) genererà dei file danneggiati: il CSS, infatti, danneggia "virtualmente" i file e il laser del lettore DVD interpreta questi errori virtuali come errori reali. Il file video restituito sarebbe un file con immagini artefatte e audio distorto (vedi figura 9).

Figura 9 Video danneggiato dal CSS

Il sistema di protezione CSS è una tecnologia di cifratura a chiavi digitali doppie a 40 bit, che agiscono in cascata (la limitata lunghezza della chiave risulta essere un punto debole di questa tecnica). Le industrie interessate a produrre dispositivi conformi al CSS devono sottoscrivere un accordo di licenza con la DVD Copy Control Association (DVD CCA). La DVD CCA rilascia alle industrie associate che fabbricano lettori DVD:

1. un attestato di licenza;
2. un numero di licenza progressivo che indichiamo con i;
3. le specifiche tecniche per la costruzione di circuiti integrati che implementano il sistema;
4. un insieme di M chiavi lettore indicato con $SetKey_i$ dove i è il numero di licenza progressivo (supponiamo che le industrie con licenza siano N quindi $1 \leq i \leq N$). Tali chiavi, indicate con $PlayerKey_j$, dove $1 \leq j \leq M$, devono essere memorizzate all'interno di un registro ROM di ogni lettore DVD prodotto. Ogni chiave lettore è lunga 5 byte, ovvero 40 bit;
5. una chiave segreta, indicata con SecretKey, di 5 byte. Questa chiave va memorizzata in un registro ROM di ogni lettore DVD prodotto e viene utilizzata dai device driver (gestore di dispositivo, software di basso livello associato ad un dispositivo di I/O preposto a gestirne la parte dipendente dall'hardware, definizione presente su "I moderni sistemi operativi" di Andrew S. Tanembaum) che vengono eseguiti sull'Host.

A settembre 2003 le industrie licenziate ammontano a 409. Supponiamo, per esempio, che un'industria sottoscriva la licenza CSS. A questo punto la DVD CCA rilascia a tale industria oltre l'attestato, le chiavi e le specifiche tecniche anche il numero di licenza 410.

Ogni DVD protetto con il sistema CSS contiene:

- i dati audio/video cifrati;
- un'area nascosta detta Hidden Area la quale viene impressa in una fase di pre-registrazione del disco tramite un particolare macchinario.

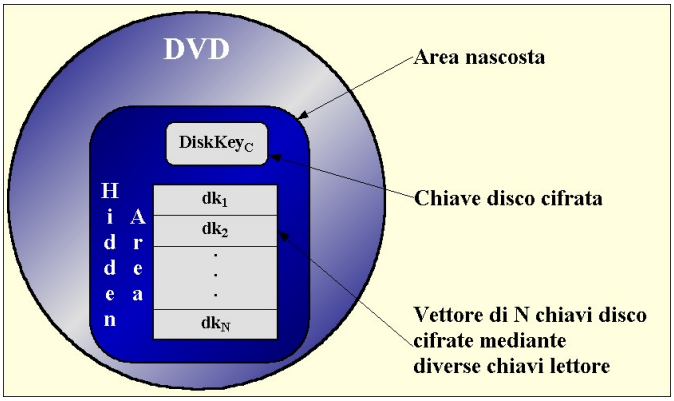

Figura 10 Contenuto della Hidden Area

Tale area contiene:

- ✓ N chiavi disco cifrate, indicate con dk_i, dove $1 \leq i \leq N$. Ogni dk_i è di 40 bit. dk_i = CSS(DiskKey, $PlayerKey_j$) dove DiskKey è la chiave del DVD e $PlayerKey_j$ è una delle M chiave lettore appartenente a $SetKey_i$.
- ✓ Una chiave disco cifrata viene indicata con $DiskKey_c$.

Un DVD contiene una serie di chiavi titolo legate ognuna ad un file VOB di dati audio/video. Poiché la dimensione di ogni file VOB non può superare la dimensione di un gigabyte, i contenuti audio/video presenti su un DVD vengono spesso divisi in una sequenza di file VOB. Le industrie che producono DVD associano ad ogni file VOB una chiave titolo TitleKey (chiave casuale di 40 bit). La chiave titolo Titlekey è presente sul DVD nel file VOB in forma cifrata indicata con $TitleKey_c$.

$TitleKey_c$ = CSS(TitleKey, DiskKey). Esiste, dunque, una chiave titolo per ogni file VOB presente sul DVD.

Riepilogando, le chiavi che vengono utilizzate dal sistema CSS sono:

- ✓ chiavi lettore (PlayerKey): queste chiavi sono rilasciate dalla DVD CCA alle industrie che fabbricano lettori DVD dopo la sottoscrizione della licenza (processo di sottoscrizione). Ognuna di queste chiavi è lunga 5 byte;

- ✓ chiave disco (DiskKey): ad ogni DVD viene associata una chiave disco DiskKey di 5 byte. Questa chiave è presente sul DVD in forma cifrata indicata con DiskKeyc;
- ✓ chiave titolo (TitleKey): ad ogni file VOB presente sul DVD è associato una chiave titolo cifrata TitleKeyc. La chiave titolo in chiaro TitleKey viene determinata mediante la chiave disco DiskKey;
- ✓ chiave settore (SectorKey): ogni file VOB presente su un DVD è costituito da uno o più settori. Ogni settore ha una dimensione di 2048 byte di dati audio/video. I primi 128 byte di dati sono in chiaro, mentre i successivi byte sono cifrati. La chiave settore SectorKey è determinata mediante un'operazione di XOR tra la chiave titolo TitleKey e 5 byte di dati in chiaro prelevati dall'intestazione del settore di 128 byte. La chiave settore SectorKey è di 5 byte.

La DiscKey e le TitleKey sono memorizzate in una piccola area nascosta del disco, detta hidden area, mentre la Player-Key è memorizzata nel lettore hardware ed è legata ad una licenza rilasciata dal produttore.

All'atto dell'inserimento del DVD-Video entro il lettore hardware, dopo una prima fase di autenticazione CSS di tipo challenge-response (che coinvolge altre chiavi), il computer richiede al lettore una porzione della DiskKey ed utilizza la PlayerKey del lettore stesso per decodificarla. Siccome esistono 409 PlayerKey, e soltanto una di esse è memorizzata nel lettore hardware, sul disco sono memorizzate 409 DiskKey, il player le prova tutte finché non trova quella corrispondente alla sua PlayerKey. Questo sistema consente di mettere fuori mercato qualunque produttore, dal momento che basterebbe non inserire più la Disk-Key corrispondente nei DVD-Video.

Dopo aver decodificato la DiskKey, il computer utilizza quest'ultima per decifrare la prima TitleKey del disco, ad essa riferita, che nel frattempo ha richiesto al lettore. Quindi, come si può intuire, nell’area nascosta vengono memorizzate N DiskKey e per ognuna di esse, il rispettivo set di TitleKey. Il canale di trasmissione è protetto tramite una SessionKey per prevenire attacchi del tipo man in the middle. A questo punto il contenuto è pronto per essere visualizzato. Quando il laser del player raggiunge un

nuovo "titolo", il computer richiede la TitleKey relativa e la decripta sempre utilizzando la DiskKey precedentemente decriptata. Il processo continua quindi, sempre grazie all'utilizzazione, in cascata, delle chiavi a due a due.

In questo documento non viene effettuato uno studio approfondito del funzionamento di questa tecnica di protezione e si delega la visione del documento “DVD e protezioni” realizzato da un gruppo di studenti dell’Università di Salerno [11].

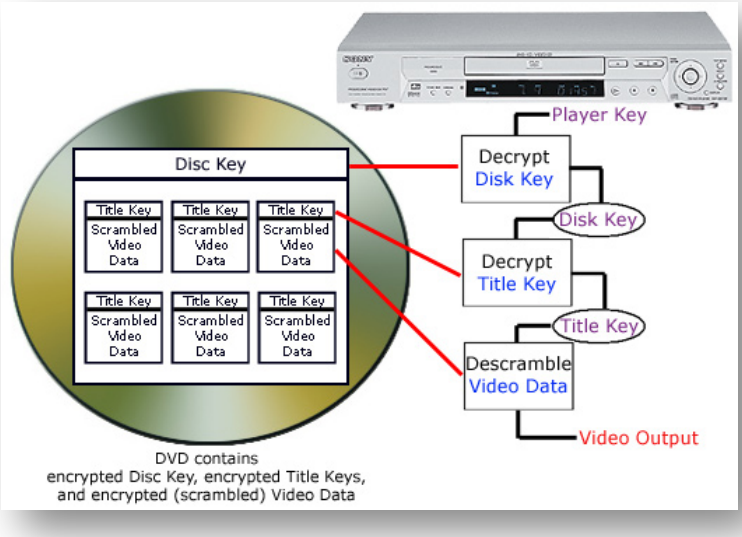

Figura 11 Visualizzare un DVD Video con CSS su un home player

2.4.3. Decrypt Content Scrambling System (DeCSS)

Il Decrypt CSS è stato ideato da tre persone norvegesi, uno dei quali è Jon Lech Johansen e le altre due sono rimaste anonime. È stato rilasciato per la prima volta su Internet sulla mailing list LiVid il 6 ottobre del 1999 (DeCSS 1.1b).

Tutto ha inizio nel 1999: i DVD, acquistati da ragazzo il cui contenuto è crittato, possono essere utilizzati su PC esclusivamente con la benedizione, certo non gratuita, delle major, in quanto i programmi impiegati allo scopo devono conoscere la chiave di decrittazione. Jon, all'epoca sedicenne, dispone di un PC sul quale è installato Linux, ma il sistema operativo libero "per eccellenza" non è stato preso in considerazione dal

business di Hollywood e, d'altra parte, chi sviluppa e distribuisce software libero non può e, giustamente, non vuole pagare balzelli: gli utilizzatori del Pinguino, in tutto il mondo, non possono che... stare a guardare (per modo di dire!).

Jon non ci sta: si mette all'opera e, utilizzando la chiave di decrittazione incorporata in chiaro da un DVD-player per Windows (XingDVD), sforna un programmino che regala a tutti la libertà di utilizzare i propri DVD senza più essere succubi dell'avida alleanza tra Signori del Software e Signori dello Spettacolo. Il programma è battezzato DeCSS e procura al suo autore un simpatico soprannome: "DVD Jon".

Com'era prevedibile, la popolarità del programma è immediata e scoppia il pandemonio. Le major, che non sanno perdere sportivamente, dapprima obbligano un webmaster americano, sotto minaccia di azione legale, a rimuovere dal suo sito un link tramite il quale era possibile scaricare DeCSS; poi denunciano gli editori di 2600 Magazine per avere pubblicato su Internet il sorgente del programma. Infine, non paghe, attraverso la MPAA (Motion Picture Association of America) esercitano pressioni sulle Autorità norvegesi per ottenere l'incriminazione dell'autore, quel piccolo mascalzone rompiscatole. A quanto pare si tratta di pressioni convincenti, perché gli eventi seguono un copione fin troppo noto: irruzione mattutina della polizia nella casa del "mascalzone", sequestro di PC e materiale correlato, denuncia, processo. Per "DVD Jon" inizia un'odissea durata quasi tre anni, terminata soltanto il 22 dicembre 2003 con un lieto fine più che meritato: assoluzione piena da tutte le accuse.

2.4.4. Content Protection for Recordable Media Specification (CPRM)

Il CPRM è stato sviluppato da IBM, Intel, Matsushita e Toshiba (collettivamente “4C”) [12]. Esso fornisce un robusto e rinnovabile metodo per la protezione dello scambio di contenuti e per la memorizzazione da parte di masterizzatori. Il CPRM è stato definito per garantire dati protetti in diversi formati memorizzati su diversi tipi di supporti fisici. Questi supporti includono: i formati DVD, le SD Memory Cards e le Secure CompactFlash.

Il CPRM è costituito da due componenti primari [28]:

- C2 cipher (Cryptomeria Cipher) [16], è un cifrario a blocchi che utilizza 10 step del cifrario di Feistel [17] ed è progettato specificamente per contenuti multimediali. Sono fornite cinque funzioni che definiscono il funzionamento del cifrario:
  - C2_E, cifratura in Electronic Codebook (ECB) Mode, come definito in ISO 8372 [29];
  - C2_D, decifratura in ECB Mode;
  - C2_ECBC, cifratura in Converted Cipher Block Chaining (C-CBC) Mode;
  - C2_DCBC, decifratura in C-CBC Mode;
  - C2_G, la funzione one-way basata su C2, mappa un valore di 56 bit e un valore di 64 bit in un valore risultato di 64 bit.
- Media Key Block si tratta della struttura dati più complessa esistente in un protetto e pre-registrato disco DVD audio e si presenta come una tabella di valori cifrati: è generata dagli esperti della 4C Entity, LLC e assegnata ai fabbricanti dei media, i quali si apprestano a memorizzarla nei file DVDAUDIO.MKB e DVDAUDIO.BUP.

Le Media Key Blocks (MKBs) sono tabelle di valori crittografici che implementano una forma di distribuzione di chiavi in broadcast, esse forniscono la rinnovabilità del sistema di protezione adottato dalle 4C. Le MKBs sono generate da 4C Entity LLC, e permettono ai prodotti con licenza di calcolare una "media key". Quando è costruito un prodotto con licenza, gli viene assegnato un insieme di "device key" (Chiavi di Dispositivo fornite dalla LLC). Le device key sono utilizzate per processare le MKBs in modo da calcolare la media key. Ci può essere un insieme unico di device key per ciascun dispositivo oppure più dispositivi possono condividere lo stesso insieme. Se un insieme di device key è compromesso in modo tale da compromettere l'integrità del sistema, vengono diffuse delle MKBs aggiornate. In questo modo le device key sono "revocate" dalle nuove chiavi. Nelle soluzioni adottate dalle 4C, le MKBs sono

memorizzate sul dispositivo di memorizzazione, i dispositivi usano la media key come la base della cifratura e della decifratura dei contenuti memorizzati sul dispositivo.

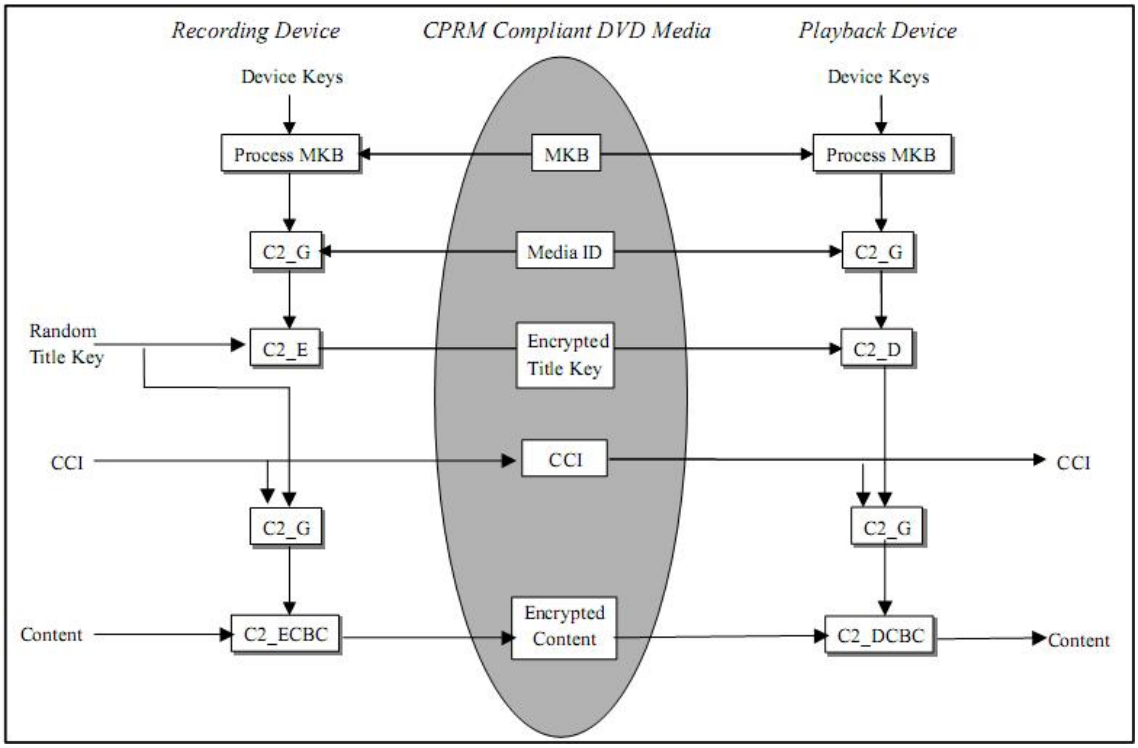

Figura 12 Funzionamento di CPRM

Ogni DVD che supporta il CPRM contiene una Media Key Block (MKB) come dato di sola lettura memorizzata in un'area protetta, e un unico Media Identifier (Media ID) memorizzato in una regione che è scrivibile una sola volta. Un registratore DVD che è autorizzato ad usare il CPRM fa una copia nel seguente modo [30]:

1. Legge il MKB dal disco (viene realizzato con la cifratura, più volte ripetute, della Media Key con le device key) ed usa le sue chiavi segrete, Device Key, per processare la MKB e calcolare la Media Key.
2. La Media Key è poi combinata con il Media ID, usando la funzione one-way C2 (C2_G), per ottenere una Media Unique Key.

3. La Media Unique Key è usata per cifrare una Title Key che è generata in modo casuale usando la funzione di cifratura del C2 (C2_E), e il valore cifrato è poi memorizzato nell'area dati del disco.
4. La Title Key è anche combinata con le Copy Control Information (CCI) usando la funzione one-way basata su C2 (C2_G), e il risultato è usato come chiave per cifrare i contenuti tramite il cifrario C2 in modalità block chaining (C2_ECBC).

Il contenuto è cifrato in modo tale che è legato ad un particolare disco, grazie all'uso del Media ID che è unico per ciascun disco. I dati protetti possono essere decifrati da un qualunque lettore DVD che è autorizzato ad usare il CPRM. Un lettore DVD usa le sue Device Key e le funzioni di decifratura di C2 per invertire il processo di cifratura. Quando viene copiato un disco protetto da CPRM, il numero seriale che contraddistingue ogni disco registrabile, diverrà parte della chiave utilizzata per criptare il contenuto: in questo modo anche se viene fatta una copia bit a bit su un altro disco vergine, il numero seriale di quel disco sarà comunque diverso da quello originale, impedendo così la decodifica del brano e dunque il suo ascolto.

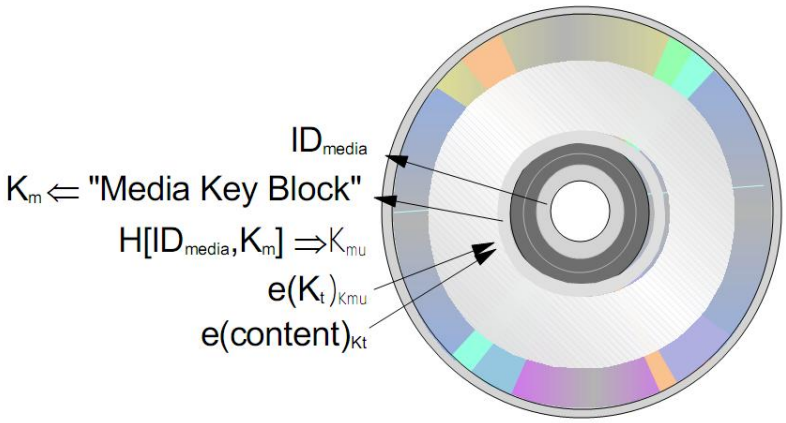

Figura 13 Organizzazione di un DVD con protezione CPRM

CAPITOLO 3: DISCHI BLU-RAY

Il Blu-ray Disc è il supporto ottico proposto dalla Sony agli inizi del 2002 come evoluzione del DVD per la televisione ad alta definizione. Grazie all'utilizzo di un laser a luce blu, riesce a contenere fino a 200 GB di dati, quasi 50 volte di più rispetto a un DVD Single Layer - Single Side (4,7 GB). Anche se questa capacità sembra enorme un disco da 25 GB può contenere a malapena 2 ore di filmato ad alta definizione utilizzando il tradizionale codec MPEG-2. Per questo motivo, oltre all'utilizzo dei dischi a doppio strato (oltre 50 GB), è stato previsto l'impiego di codec più sofisticati come l'MPEG-4 AVC o il Windows Media Video 9 (standardizzato come VC-1) che permettono in teoria di raddoppiare il fattore di compressione rispetto all'MPEG-2 (quindi dimezzando la richiesta di spazio) senza incidere significativamente sulla qualità video.

È stato utilizzato il termine Blu (usato in italiano), al posto del corretto Blue, perché di uso comune nella lingua inglese (e quindi non registrabile come marchio). Il primo apparecchio ad aver utilizzato commercialmente questa tecnologia è stata la PlayStation 3, dopo che il 12 agosto 2004 i produttori impegnati nel progetto Blu-ray dichiararono di aver approvato la versione 1.0 delle specifiche per i dischi BD-ROM. La presentazione ufficiale del nuovo supporto disponibile per il cinema ad alta definizione è avvenuta il 23 maggio 2006 negli Stati Uniti.

Il 19 febbraio 2008 il Blu-ray ha definitivamente vinto la sua competizione con l'HD DVD, visto che Toshiba, titolare dei diritti sullo standard concorrente, ha dichiarato la chiusura del progetto e la dismissione delle attività ad esso legate (chiusura probabilmente determinata anche dall'abbandono del supporto da parte di nomi come Warner Bros e Wal-Mart).

Figura 14 Esempio di disco Blu-ray

3.1. Protezione dei dati

Sul fronte della sicurezza dei dati contro la contraffazione, Blu-ray utilizza l'Advanced Encryption Standard (AES) con chiavi a 128 bit che cambiano ogni 6 Kb di dati. In una conferenza del 2004, Sony ha mostrato come una singola chiave veniva utilizzata per decriptare un video protetto, facendo notare che la chiave cambiava centinaia di volte durante la riproduzione. Il protocollo di gestione dei contenuti digitali funzionerà in cooperazione con il protocollo High-Bandwidth Digital Content Protection (HDCP)[34] per impedire la riproduzione a dispositivi non abilitati.

Il Blu-ray utilizza 3 meccanismi di protezione dei dati. Il primo è l'AACS, evoluzione del Content Scrambling System (CSS) utilizzato per i DVD. L'AACS cripta i dati veri e propri e può essere decodificato solamente conoscendo le apposite chiavi rilasciate ai produttori di player. L'AACS, quindi, di fatto serve ad impedire la riproduzione di dischi da parte di dispositivi non autorizzati o contraffatti (e che quindi potrebbero illegalmente trasferire il contenuto del supporto verso altri sistemi).

Un secondo meccanismo di protezione è quello del Digital Watermarking. Praticamente nel disco vengono inserite delle "impronte" realizzate mediante opportune modifiche

della forma dei bit, invisibili all'occhio umano, ma il cui schema può essere intercettato e ricostruito dal player durante la riproduzione. Se il player non individua lo schema, il disco viene identificato come contraffatto e non riprodotto. Il Digital Watermarking, quindi, serve ad impedire la riproduzione di dischi prodotti illegalmente.

Il terzo sistema è chiamato BD+ e si basa su una macchina virtuale che può essere eseguita nel riproduttore di Blu-ray Disc utilizzando un codice sorgente registrato direttamente nei supporti pre-registrati. Al momento del caricamento del disco, il codice viene estratto e portato nella memoria del player, dove viene eseguito. Il codice permette di decodificare il materiale registrato sul disco che è stato modificato applicando un secondo livello di protezione, aggiuntivo rispetto all'AACS, e che prevede la sostituzione di porzioni di dati utili con porzioni di dati non significative. Se tali porzioni non vengono ripristinate, il materiale risulta corrotto e quindi non leggibile. Il programma eseguito dalla macchina virtuale del BD player, si occupa appunto di ricostruire il flusso corretto di bit, permettendo la lettura del disco. Il BD+ offre due meccanismi molto potenti di protezione: innanzitutto il codice non risiede mai permanentemente nel player, in quanto non appena viene estratto il disco, la memoria della Virtual Machine viene azzerata.

La combinazione dei 3 meccanismi di protezione è considerata molto più sicura rispetto al solo AACS utilizzato per l'HD DVD.

3.1.1. AACS

L'Advanced Access Content System (AACS) è uno standard per la distribuzione e la gestione di contenuti digitali, nato per permettere una restrizione all'accesso e alla copia dei dischi ottici Blu-ray e HD DVD. Gli sviluppatori sono: Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Brothers, IBM, Toshiba e Sony ed è stato realizzato dalla AACS LA. Le specifiche furono rilasciate nell'aprile del 2005.

Il sistema include anche l'Image Constraint Token e il Digital Only Token. Si tratta di marcatori presenti sui due supporti che governano le uscite analogiche del lettore, siano

esse di tipo component, video composito, S-Video, SCART e VGA. L'attivazione del Digital Only Token oscura completamente l'output analogico, forzando la riproduzione unicamente attraverso una connessione digitale protetta con HDCP. L'attivazione del flag Image Constraint Token istruisce il lettore a ridimensionare la risoluzione video al valore massimo di 960x540 pixel, esattamente un quarto della risoluzione definita Full Hd di 1920x1080 pixel. Nei seguenti paragrafi verranno analizzati i componenti del sistema AACS

Volume ID

I Volume IDs sono identificatori unici o numeri di serie che vengono memorizzati sui dischi tramite una pre-registrazione attraverso un hardware speciale. Il suo utilizzo è per evitare la semplice copia bit-a-bit, in quanto il Volume ID è necessario (anche se non sufficiente) per la decodifica dei contenuti. Nei dischi Blu-ray, il Volume ID viene memorizzato nella BD-ROM Mark (uno strato fisico dei dischi Blu-Ray non copiabile dai normali masterizzatori ma solo da sofisticati hardware).

Per leggere il Volume ID è necessario un certificato (la chiave privata Host), firmato dalla AACS LA rilasciato nel momento in cui la casa produttrice di player effettua l'iscrizione presso la AACS LA. Tuttavia, gli hacker dichiarano di aver aggirato la protezione modificando il firmware di un lettore HD DVD.

Device Key

Ogni dispositivo compatibile con AACS ha una serie di DeviceKey [32] e vengono rilasciate dalla AACS LA. Sono utilizzate dal dispositivo per processare i Media Key Block (MKB) per calcolare l'insieme delle DeviceKey univoche per ogni dispositivo.

I Media Key Block (MKB)

Anch'esso viene generato dalla AACS LA e permette al dispositivo la generazione dell'insieme del DeviceKey. Se un insieme di DeviceKey è compromesso, in modo tale da attentare l'integrità del sistema, verrà diffuso un MKB aggiornato, così che un dispositivo con chiavi compromesse non sia più in grado di calcolare la corretta MediaKey: le DeviceKey compromesse sono revocate dal nuovo MKB. Un MKB è configurato come una sequenza di Record contigui.

Gestione ad albero delle chiavi

La motivazione che ha condotto alla nascita di questo nuovo schema va ricercata nel fatto che gli schemi precedentemente visti (CPRM), basati su matrici, presentavano principalmente due lati negativi:

- ✓ è scomodo e non completamente soddisfacente pensare ad una crescita del numero di revoche, una volta che il sistema è stato schierato (in termini di dimensione delle matrici);
- ✓ il sistema è particolarmente sensibile agli attacchi di un membro: si tratta del cosiddetto problema del fabbricante diabolico, in cui un fabbricante autorizzato fa un uso illecito delle sue chiavi;

Subset Difference Method permette di partizionare l'insieme degli utenti autorizzati in maniera più efficiente; i riceventi però, saranno gravati da un maggior carico computazionale in fase di decodifica.

In un tale schema, gli utenti sono visti come foglie di un albero binario completo di radice r_a. La collezione di sottoinsiemi S_1, S_2, …, S_w definiti da questo algoritmo, corrisponde a sottoinsiemi della forma "un gruppo di utenti G_1 meno un gruppo di utenti G_2" , dove $G_2 \subset G_1$: i due gruppi G_1 e G_2 corrispondono a foglie in due sottoalberi binari pieni. Un valido sottoinsieme S è rappresentato attraverso due nodi dell'albero (v_i, v_j), tali che v_i (radice principale) è un antenato di v_j (radice secondaria): denotiamo un tale sottoinsieme S_{ij} - meglio noto come insieme differenza.

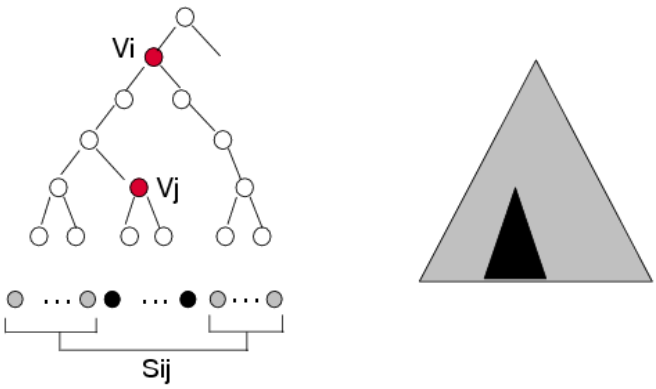

Figura 15 Rappresentazione dell'insieme differenza

L'MKB è una struttura ad albero in grado di gestire la pubblicazione e la revoca delle chiavi. Il sistema si basa su un gran numero di master tree di chiavi, dove ogni dispositivo è associato ad una foglia dell'albero e ogni dispositivo riceve un insieme di DeviceKey.

Tramite l'uso di questa tecnica, è possibile effettuare una revoca sia individualmente che per un vasto insieme di dispositivi.

Processing Key

La processing key, ovvero la "chiave universale" capace di decodificare tutti i film Blu-ray distribuiti fino ad oggi sul mercato. Mentre le volume key cambiano da film a film, e talvolta da lotto a lotto, la processing key è una sorta di passepartout con cui è possibile sbloccare, decifrare e fare il backup di ogni film rilasciato fino ad oggi e protetto con la tecnologia AACS.

Cifratura

AACS crittografa i contenuti in una o più TitleKey utilizzando Advanced Encryption Standard (AES). Le TitleKey sono derivati da una combinazione di un supporto chiave (codificato tramite un Media Key Block) ed un Volume ID del supporto (ad esempio, un numero di serie fisico incorporato e pre-registrato nel disco).

La principale differenza tra AACS e CSS, il sistema DRM utilizzato su DVD, si trova nel modo in cui il dispositivo organizza le chiavi per la decodifica.

Tramite CSS, tutti gli home player di un determinato modello hanno le stesse chiavi condivise per la decifratura. Il contenuto è cifrato tramite la specifica TitleKey la quale è a sua volta cifrata tramite la chiave di ciascun modello. Pertanto ogni disco contiene una raccolta di alcune centinaia di chiavi cifrate, uno per ogni modello di player che ha la licenza.

Inizialmente, questo approccio permetteva ai possessori della licenza di revocare un determinate modello (in modo da impedire in futuro la riproduzione) omettendo in futuro la cifratura delle TitleKey per quel modello. In pratica, tuttavia, la revoca di tutti

i player di un determinate modello è costoso, in quanto molti utenti perdono la capacità di riproduzione.

Lo standard consente a diverse versioni di brevi sezioni di un film ad essere codificato con chiavi diverse. Un player sarà in grado di decifrare una versione di ogni sezione.

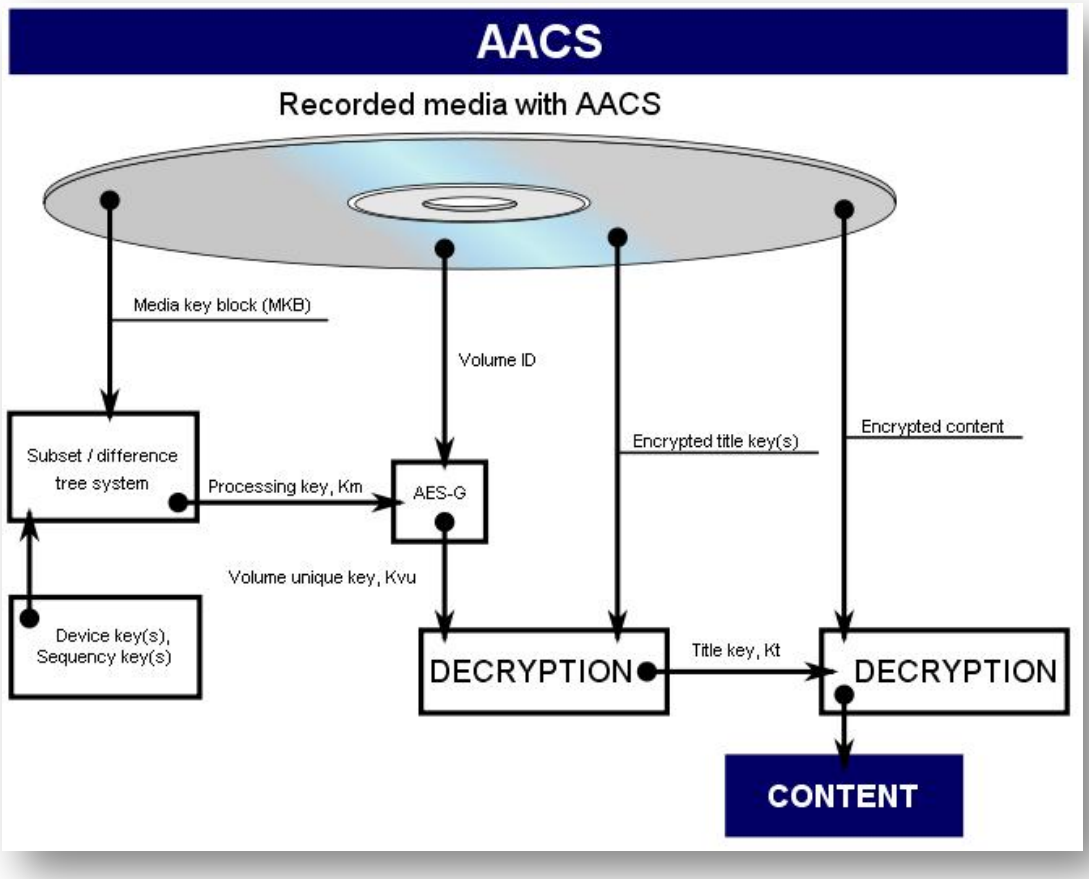

Figura 16 Fase di decifratura del sistema AACS

Processo di decodifica

La figura 16 mostra il funzionamento della fase di decifratura.

Per visualizzare il filmato [31], il giocatore deve prima decifrare il contenuto del disco. Il disco contiene 4 elementi:

- Media Key Block (MKB);
- il Volume ID;
- la TitleKey cifrata;
- il contenuto cifrato.

Il MKB è codificato in un differente sottoinsieme ad albero. In sostanza, una serie di chiavi sono disposti in un albero in modo che ogni chiave può essere utilizzata per trovare ogni altra chiave, eccetto la sua chiave madre. In questo modo, per revocare una determinata chiave di un dispositivo, basta che l'MKB venga crittografato solo con la sua chiave madre.

Una volta che il MKB viene decifrato, si ottiene la MediaKey o la chiave master. La chiave master è combinata con il volume ID (che il programma può ottenere solo presentando un certificato di cifratura per il dispositivo, come descritto in precedenza), tramite uno schema di cifratura (AES-G) ottenendo cosi il VolumeUniqueKey (Kvu). Il Kvu viene utilizzato per decifrare le TitleKey le quali vengono utilizzate per decifrare il contenuto cifrato.

Sia le TitleKey che una delle chiavi per decifrarle sono state trovate utilizzando il debugger per controllare lo spazio di memoria in esecuzione dei programmi per i dischi Blu-ray. Il problema sta nel fatto che le chiavi risiedono nella memoria del PC e gli hacker hanno sfruttato proprio la lettura della memoria per ottenere cosi le chiavi per la decifratura. L'unico modo per prevenire questo attacco sarebbe quello di modificare la piattaforma del PC per prevenire gli attacchi.

La prima notizia di forzatura di questo sistema è stata pubblicata il 18 dicembre 2006 da parte dell'hacker "Muslix64": con il suo programma BackupHDDVD è riuscito a trovare le TitleKey di protezione dei film, prima in HD DVD e successivamente in Blu-ray (sebbene senza protezione BD+). L'hacker ha dichiarato che per prendere le chiavi non ha fatto altro che sfruttare le debolezze di alcuni lettori multimediali che memorizzano le chiavi nella RAM senza cifrarle, ma non ha reso pubbliche le chiavi utilizzate.

Un frequentatore del forum di Doom9.org ha trovato dapprima la DeviceKey del lettore WinDVD e a marzo di PowerDVD. Nel febbraio 2007 è stato trovato il modo di ottenere le volume key di ogni singolo film Blu-Ray.

Nel mese di febbraio l'hacker Arnezami ha scoperto la "processing key" per decodificare tutti i dischi Blu-ray prodotti fino al 2007 protetti con AACS. Il consorzio AACS ha tentato di limitare la diffusione della chiave, causando una sua diffusione capillare.

Il 23 maggio 2007 Arnezami ha trovato la nuova processing key adottata dall'industria cinematografica pubblicandola nuovamente sul forum di Doom9.org

3.1.2. Digital Watermarking

Il Digital Watermarking [14] è una tecnica mediante la quale un'informazione (watermark) viene inserita all'interno di un documento digitale (audio, video, immagine, ecc..) con i seguenti obiettivi:

- ✓ recare le informazioni di copyright, per proteggere i diritti d'autore in ambito commerciale;
- ✓ dimostrare l'autenticità di un documento, cioè che il documento è allo stato originale e non è stato manomesso o modificato;
- ✓ impedire le copie non autorizzate e permettere quelle consentite, inserendo informazioni di controllo copia;
- ✓ identificare un distributore non autorizzato, inserendo nel watermark anche il nome del compratore del documento, al momento della vendita.

In realtà, non è semplice stabilire quali tecniche rientrino nella dicitura "watermarking". In alcuni casi si effettua una distinzione tra "fragile watermarking" e "watermarking"; e per quest'ultimo si fa ancora una distinzione tra "imperceptible watermarking" e "visible watermarking".

Il watermark è un marchio “trasparente”. Risulta quindi difficile immaginare un marchio trasparente ma visibile, che è quello che dovrebbe incontrarsi nel caso di “visible watermarking”. Tuttavia, in questo caso il marchio è rappresentato da un logo sovrapponibile ad un immagine o ad un filmato, in maniera poco evidente rispetto a quelli che sono i loghi tradizionali. Tali loghi risultano essere sparsi su tutta l'immagine e difficilmente rimovibili. Gli aggettivi fragile e robusto stabiliscono in maniera netta qual è il fine del watermark. I watermark “fragili” sono concepiti per quelle applicazioni in cui si desidera sapere se una certa informazione è stata modificata nel passaggio dal creatore all'utilizzatore, nel qual caso il watermark deve distruggersi, nel senso di non essere rilevabile o comunque deve presentare alterazioni; si tratta dunque di una sorta di impronta elettronica, che, a differenza di quelle tradizionali, è incorporata nell'informazione stessa da proteggere. Al contrario, i watermark “robusti” devono ottenere la massima resistenza a tutta una serie di attacchi, minimizzando più che le modifiche all'originale, l'impatto visivo di queste, e raggiungere perciò un obiettivo opposto; l'informazione che essi trasportano all'interno dell'originale non deve perdersi e deve potersi recuperare, anche se l'originale è modificato. Il watermarking deve inoltre essere resistente a delle operazioni come la conversione digitale-analogico, la ri-quantizzazione, il ri-campionamento, il cambio di scala, la distorsione, la traslazione e la compressione. Particolare attenzione meritano, per il problema della ridistribuzione via Internet, la conversione digitale-analogico-digitale e la compressione. E’ quindi chiaro che mediante il watermarking è possibile costruire un sistema DRM ma non solo, con esso si soddisfa l’esigenza di riuscire a stabilire la provenienza del materiale che si utilizza.

3.1.3. BD+

La protezione BD+ è formata da due componenti: una risiede sul supporto Blu-ray ed è un programma, la seconda componente è una macchina virtuale che risiede sul lettore Blu-ray e che esegue il software memorizzato nel disco. Questo permette ai produttori

di includere dei contenuti interattivi e di includere delle nuove tecnologie di protezione direttamente nel supporto.

I programmi prima di essere eseguiti provvedono ad effettuare le seguenti operazioni:

a. esaminano il lettore Blu-ray al fine di verificare eventuali manomissioni. Ogni produttore di lettori Blu-ray ha anche una licenza per la tecnologia DB+ che viene memorizzata nel lettore e serve a verificare l'autenticità del dispositivo;
b. verificano che la chiave di decodifica del lettore non sia stata manomessa;
c. eseguono il programma memorizzato sul disco e tamponano eventuali problemi di sicurezza del lettore,
d. decodificano i flussi audio e video.

BD+ fa girare sui lettori una sorta di Virtual Machine non appena un disco viene inserito. Una volta caricata, la VM estrae dal disco un codice addizionale, eseguendo una triplice funzione:

- ✓ la prima è quella di trasformare porzioni di video deliberatamente corrotte rendendole visibili in modo corretto; se infatti il film Blu-ray fosse "rippato" risulterebbe danneggiato in molte sue parti.
- ✓ la seconda funzione è quella di poter patchare il firmware di lettori su cui risultano manomissioni o hack, di fatto revocando la licenza delle chiavi di lettura e rendendo impossibile l'utilizzo dei futuri dischi inseriti.
- ✓ l'ultima funzione del codice è quella di aggiungere un watermark al disco, ovvero una informazione di copyright nascosta utilizzabile a fini investigativi, per quanto riguarda i reati di sofisticazione digitale.

La figura 17 mostra il funzionamento di BD+ e come i flussi video vengono decodificati.

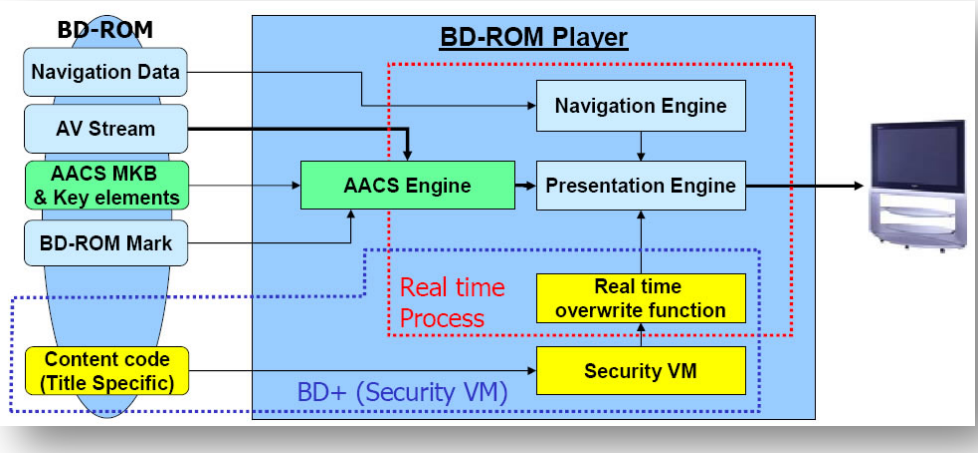

Figura 17 Fuzionamento di BD+

Una volta che i dischi BD+ sono estratti dal lettore, la virtual machine viene scaricata dalla memoria interna e il player torna al suo stato originale, cosicché se la macchina fallisse la lettura di questi nuovi dischi, sarebbe comunque in grado di leggere i "vecchi" film Blu-ray che non contengono la protezione BD+.

Secondo la Blu-ray Disc Association (BDA), raggirare la protezione della virtual machine sarà una difficile impresa per gli hacker, in quanto effettuare operazioni di reverse-engineering sul codice risulta molto più complicato rispetto all'acquisizione delle chiavi che costituiscono la protezione base di ogni BD.

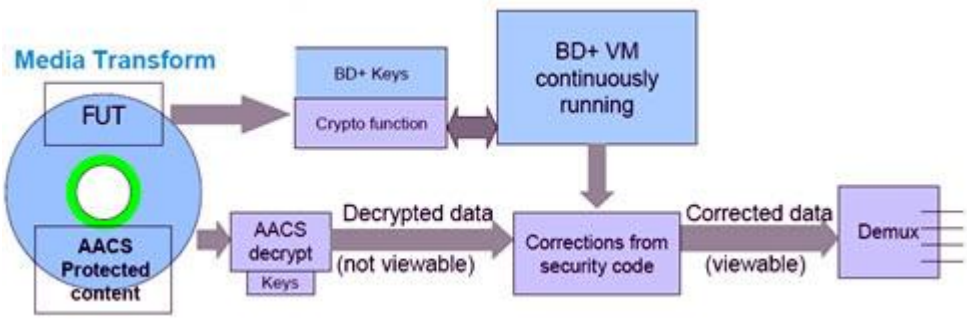

Figura 18 Macchina virtuale di BD+

In caso di copia di un disco Blu-ray, solo il contenuto cifrato verrà copiato, mentre le informazioni contenute nel BD-ROM non possono essere copiate dai normali masterizzatori ma solo da particolari e costosissimi macchinari. A causa di ciò, un lettore non riesce a riprodurre il contenuto in quanto non riesce a decifrarlo (Figura 19). L'implementazione della tecnologia BD+ non significa però solo protezione maggiore. Per la sua stessa natura, BD+ è un codice e come tale può far girare sulla Virtual Console ogni sorta di limitazione o disposizione a piacimento dei produttori. Questo significa, ad esempio, uscite "a tempo" oppure dischi che diventano inutilizzabili dopo un dato numero di volte.

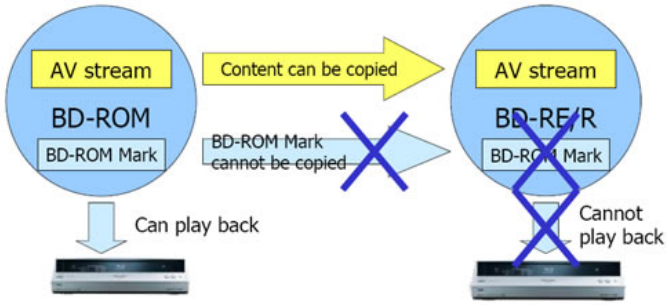

Figura 19 Comportamento della tecnica BD+ in caso di copia

Il 30 ottobre 2007 Slysoft ha annunciato di essere riuscita a forzare il BD+ e il 19 marzo 2008 è uscita la versione del software che permette la copia di dischi Blu-Ray codificati con la tecnica BD+.

Per aggirare BD+, gli hacker si sono avvalsi di complesse tecniche di debugging e di un lettore Blu-ray con il firmware modificato. Questo ha permesso loro di sfruttare la tecnologia di virtualizzazione per ricreare una macchina virtuale BD+, la stessa che i player eseguono ogni volta che viene riprodotto un disco Blu-ray protetto.

CAPITOLO 4: SONY BMG

Le tecnologie Digital Right Management sono realizzabili da un lato, mediante la cifratura dei contenuti e la distribuzione a pagamento delle chiavi di apertura di contenuti coperti da diritto d'autore, dall'altro come un sistema che non si limita a presidiare gli aspetti di sicurezza, rispetto ad accessi o duplicazioni illegali, ma sovrintende sulla descrizione, identificazione e protezione di tutte le forme di cessione del diritto, all'uso di uno specifico contenuto.

Molte società hanno tentato di applicare le tecnologie DRM nei più svariati modi, a volte senza riuscirci, in altre finendo al centro di un turbinio di polemiche, su come potessero essere applicate senza violare la privacy e la libertà degli utenti. I cd oggi distribuiti devono tutti gestire la musica in formato Compact Disc Digital Audio (CDDA), l'unico che consente a tutti i lettori in circolazione di leggere quelle tracce. Se la musica è inserita sul disco in un formato che qualsiasi software deve poter leggere, l'unico modo per impedire ai programmi di leggerlo è installare del software sul computer dell'utente e di far sì che interferisca attivamente con i tentativi di accedere al disco, ad esempio, corrompendo il flusso di dati che viene dal disco. Questa protezione è chiamata "protezione attiva".

Il problema, evidentemente, è che l'utente non vuole questo genere di software, non vuole installarlo e lo rifiuta perché non gli fornisce alcun valore aggiunto, anzi, riduce la sue libertà. Questo significa che se si vuole realizzare un sistema DRM per i cd, basato sulla protezione attiva, ci sono due questioni da risolvere:

1. far sì che l'utente installi il software, anche se non vuole;
2. una volta installato, occorre impedire che venga disinstallato, anche se l'utente non vuole.

La conseguenza sarà il ricorso ad un software che deve potersi installare ad insaputa dell'utente.

Le finalità dei sistemi di Digital Right Management (DRM) sono tali che, indipendentemente dalle tecnologie utilizzate, sono destinate a rivelarsi spyware e a proporsi in modo sempre più invasivo, trovando, nell'ingannare l'utente, la via per diffondersi. Questa è l'accusa ribadita da Ed Felten, celebre professore di Princeton da anni impegnato nello studio delle tecnologie di protezione dei contenuti, contro la Sony BMG: il gigante nipponico è accusato di installare software all'insaputa degli utenti.

Figura 20 Logo Sony BMG

A scatenare il caso mediatico è stato Mark Russinovich del gruppo SysInternals. Russinovich ha scoperto quasi per caso il funzionamento della nuova tecnologia DRM di Sony BMG, inserita in alcuni cd in vendita probabilmente già da marzo 2005: ha infatti individuato per caso, un software nascosto sul proprio computer. Sul blog tecnico di Russinovich [18], vengono analizzate punto per punto le tecniche utilizzate dal software per intrufolarsi in Windows, tecniche paragonabili a quelle di moltissimi spyware.

Svolgendo alcune indagini è emerso che tale applicazione era stata installata dal meccanismo di protezione eXtended Copy Protection (XCP), un sistema utilizzato nei cd Sony BMG per combattere la pirateria. Quello che viene contestato è che il software si installa di nascosto, non dispone di una procedura di rimozione ed è mal realizzato: questo si traduce in frequenti rallentamenti del sistema; per di più, tentando la rimozione forzata del software, il drive del CD-ROM sparisce del tutto. A fronte di questa serie di comportamenti quindi, non è stato difficile etichettare il programma come un rootkit: XCP.Sony.Rootkit.

Un rootkit è una raccolta di tool che un intruso installa sulla macchina vittima dopo essersi guadagnato un accesso non autorizzato alla stessa. La sua caratteristica fondamentale è quella di risultare totalmente invisibile al sistema, in modo che né l'utente, né nessun programma possano identificarlo. Per fare ciò, parlando del sistema operativo Windows, un rootkit può seguire due diverse strade: una è quella di intercettare le chiamate alle API di Windows e modificandole arbitrariamente, cerca di non farsi identificare; un'altra è quella di modificare il comportamento del kernel di sistema (Kernel-mode Rootkit).

I rootkit non si vedono, controllano i programmi in esecuzione e non si notano, però ci sono. E' divenuto presto evidente come il rootkit della BMG stava spiando le azioni dei propri utenti e mandava un profilo degli stessi ai server della casa discografica.

I cd audio, prodotti e commercializzati da Sony BMG, non contengono solo musica: sono in realtà cd ibridi; dispongono di una parte dati leggibile dal computer, riferita ad un software per la prevenzione della copia denominato eXtended Copy Protection (XCP), sviluppato dalla compagnia inglese First4Internet.

Quando un disco protetto XCP viene inserito in un PC, l'autorun di Windows lancia un installer XCP, precisamente il file go.exe. L'installer visualizza una licenza, la EULA (End User License Agreements). Se l'utente decide di non accettare la licenza, il software non sarà installato. Diversamente, accettando tale licenza, la funzione di autoplay di Windows manderà automaticamente in esecuzione l'installazione di questo software, presentato all'utente come "un semplice player necessario per utilizzare il disco". In realtà, oltre a lanciare un player (Music Player), l'unico che consentirà l'ascolto o l'estrazione delle tracce sull'hard disk, nonché la duplicazione limitata del disco, farà qualcosa di molto più profondo: installa un processo che lavora in background e che si interpone tra le applicazioni e il driver originale del cd; in tal modo si sostituisce ai normali device driver di gestione del cd per poter attuare le limitazioni alla copia ed imporre altre funzioni di "prevenzione degli illeciti".

Dopodiché, per evitare che l'utente possa tentare di inibire o disinstallare tali funzioni di limitazione, il programma di installazione provvede a rendere invisibili i device driver appena installati, utilizzando le tecniche di cloaking tipiche dei rootkit.

Il software DRM installa due servizi DRM come servizi di Windows, avviati automaticamente durante lo startup del sistema:

1. XCP CD Proxy
2. Plug And Play Device Manager

In particolare quest'ultimo monitorizza i programmi in esecuzione sul computer; approssimativamente ogni 1,5 secondi, interroga gli eseguibili associati a tutti i processi in esecuzione (proprio come un programma malware) con conseguenti tentativi di lettura sul disco fisso: questo naturalmente si traduce in un utilizzo smodato della CPU e un conseguente rallentamento del sistema. Per la descrizione più approfondita del funzionamento del software, si consiglia la visione del documento *"Nuove tecniche DRM per la protezione di copia" [20]*.

4.1. Obiettivi e funzionamento di XCP

La tecnologia anticopia XCP consente agli utenti di copiare i dischi protetti un numero limitato di volte (tre per la precisione), impedendo del tutto la generazione di copie funzionanti di cd non originali.

Essa prevede un sistema proprietario di Digital Right Management e parte dal presupposto che le copie di un cd protetto siano "sterili", ovvero, a partire da esse, non sia possibile generare ulteriori duplicati (sterile burning); limita inoltre l'estrazione delle tracce audio sul proprio hard disk mediante un apposito programma fornito in dotazione, che mette sotto chiave la musica copiata su disco, in modo che possa essere riprodotta solo con la corretta licenza. Il caso apre diverse discussioni, soprattutto di tipo legale: il software in questione appare molto simile ai comuni spyware, ed è progettato affinché contatti il sito web del fornitore ogni qualvolta l'utente inserisce un

disco protetto: l'obiettivo potrebbe essere quello di permettere il download di immagini o annunci pubblicitari mentre si sta ascoltando la musica, ma anche, e soprattutto, quello di osservare le abitudini musicali dell'utente: fenomeno noto con il nome di Phoning Home. Nonostante la Sony BMG e la First4Internet sostengano che la presenza del rootkit non sia pericolosa e che tutto sia regolare secondo i loro canoni, hanno rilasciato due patch capaci, a loro avviso di rimuovere l'applicazione; un'attenta analisi ha però evidenziato serie vulnerabilità ai sistemi che le hanno utilizzate.

Quando un CD con tale protezione veniva ascoltato su un normale lettore non vi era alcun problema; per ascoltarlo sul computer era, al contrario necessaria una procedura atipica: il CD lanciava un player, un nuovo player, l'unico capace di permettere l'ascolto dello stesso CD. Con l'installazione di questo player, veniva installato anche il software spia, software capace di impedire la duplicazione di quella musica ma anche di inviare informazioni alla Sony.

Non solo: per fare questo, la spia era capace di distruggere le protezioni del PC, che a quel punto sarebbe stato a disposizione di qualunque pirata informatico; per di più, il software spia non aveva dentro di sè nessuna informazione che potesse guidare alla sua disinstallazione, doveva restare lì.

Figura 21 Come il player della Sony si presentava all'utente

Una volta che il software DRM è installato, ogni volta che un nuovo cd viene inserito, i filter driver eseguono un algoritmo di riconoscimento del disco e se riconoscono che il disco detiene un tale schema DRM, interferiscono su qualsiasi tentativo di lettura delle tracce audio presenti sul disco, effettuato da parte di un processo che non sia il Music Player (player.exe) corrompendo l'audio ritornato dal drive e sostituendo questo flusso di dati con del rumore casuale.

Il rootkit chiama le funzioni reali del kernel con gli stessi parametri, e filtra i risultati prima che loro ritornino all'applicazione. Il rootkit re-dirige cinque funzioni Native API, precisamente la :

- ✓ NtCreateFile: Crea e apre file. Il rootkit ritorna un "invalid filename error" quando le applicazioni tentano di aprire un file il cui nome inizia con sys;
- ✓ NtEnumerateKey: Ritorna una lista di sottochiavi di una chiave di registro. Filtra i risultati rimuovendo le sottochiavi il cui nome inizia con sys;
- ✓ NtOpenKey: Apre una chiave di registro. Potrebbe filtrare le chiavi di registro che iniziano con sys, rendendole invisibili al sistema;
- ✓ NtQueryDirectoryFile: Lista i contenuti di una directory. Il rootkit filtra le entrate che iniziano con sys, rendendo file e directory invisibili al sistema.
- ✓ NtQuerySystemInformation: Lista i processi in esecuzione. Il rootkit filtra i processi i cui nomi iniziano con sys, rendendoli invisibili al sistema.

Il rootkit nasconde file, processi o chiavi di registro, il cui nome inizia con sys: questo rappresenta una seria vulnerabilità, dal momento che potrebbe potenzialmente nascondere anche file o processi di un attaccante, una volta che l'accesso al sistema infettato è avvenuto. E' evidente come XCP.Sony.Rootkit modifichi il sistema operativo a basso livello e come ciò rappresenti una grande minaccia per l'integrità dei sistemi degli utenti. Se si tenta, tra l'altro, una rimozione manuale, l'accesso al CD-ROM dell'utente sarà disabilitato proprio a causa della mancanza dei filter driver. Nessuna procedura disinstallante è inclusa con il software XCP.Sony.Rootkit: la Sony BMG ha rilasciato una patch, ma, è stato evidenziato come essa introduca una seria vulnerabilità al sistema sul quale è eseguita.

Il software della Sony si propone di impedire la generazione di copie funzionanti a partire dai duplicati del cd originale, limitando ad un massimo di tre, il numero di copie generabili a partire da quest'ultimo: le copie sono effettuabili solo attraverso l'applicazione burning proprietaria fornita dal Music Player della Sony.

Quest'ultima si avvale della tecnica Copy Generation Management System (CGMS) [19]. Il sistema lavora memorizzando due bit di CGMS Copy-Control Information (CCI) nel'header del disco: si tratta di un'informazione aggiunta allo stream di dati che contiene la musica, ogni qualvolta viene fatta una copia digitale.

La Sony BMG, inoltre, limita l'estrazione delle tracce sull'hard disk solo con lo speciale software fornito in dotazione con i dischi: i dischi, permettono di copiare i file audio sul computer dell'utente in un formato audio protetto da DRM.

L'utente può estrarre le tracce sull'hard disk solo in un formato audio protetto: in particolare potrà scegliere di copiare le tracce in un formato Windows Media Audio e questo può avvenire grazie al Windows Media Data Session Toolkit (WMDST) che consente ai discografici di creare dei cd ibridi contenenti, in sessioni separate, diverse versioni dello stesso album.

Il WMSDT consente difatti di trasportare le licenze DRM emesse dal Windows Media Rights Manager limitate al PC sul quale le tracce sono estratte, e tali da permettere o la copia su cd o il trasferimento della musica su device portatili che supportano la piattaforma Windows Media DRM: i Windows Media file non potranno però essere ascoltati se copiati su altri PC, in quanto le restrizioni DRM ne inficiano l'utilizzabilità. Il processo di base del funzionamento di WMDRM si articola nelle seguenti fasi:

1. creazione del pacchetto. Il Windows Media Right Manager crea un pacchetto per il file multimediale digitale. Il file viene crittografato e bloccato con una chiave, che viene memorizzata in una licenza cifrata, distribuita separatamente. Al file multimediale digitale vengono aggiunte altre informazioni, ad esempio l'URL per l'acquisizione della licenza. Il file multimediale digitale risultante

viene salvato nel formato audio Windows Media (file con estensione wma) o nel formato video Windows Media (file con estensione wmv).

2. distribuzione. Il pacchetto viene distribuito su cd.
3. acquisizione delle licenze. Per riprodurre un file multimediale digitale crittografato, l'utente deve prima ottenere la chiave di licenza con cui sbloccare il file. Il processo di acquisizione di una licenza inizia automaticamente quando l'utente cerca di acquisire il file multimediale digitale crittografato, quando acquisisce una licenza consegnata anticipatamente o quando riproduce il file per la prima volta.
4. riproduzione del file multimediale digitale. Per riprodurre il file multimediale digitale, è necessario un lettore che supporti Windows Media DRM. Il file potrà essere riprodotto secondo le regole o i diritti inclusi nella licenza. Le licenze possono avere diritti diversi: ad esempio, i diritti predefiniti potrebbero consentire all'utente di riprodurre il file multimediale digitale su un computer specifico e copiarlo su un dispositivo portatile. Le licenze, tuttavia, non sono trasferibili. Se un utente invia un file multimediale digitale crittografato a un amico, questi deve acquisire una sua licenza per poter riprodurre il file multimediale digitale. Questo modello di assegnazione della licenza PC, per PC, offre la certezza che il file multimediale digitale crittografato venga riprodotto solo dal PC a cui è stata assegnata la chiave di licenza relativa al file in questione.

4.2. Aspetti negativi della tecnologia XCP

Il comportamento della tecnologia eXtended Copy Protection è stato paragonato in tutto e per tutto a quello di un virus: si installa di nascosto, nasconde file, processi, chiavi di registro e non dispone di una procedura di rimozione. Il software in questione monitorizza continuamente l'attività del computer dell'utente, un riferimento piuttosto inesatto per essere una funzionalità di un software DRM: secondo alcuni esperti, effettua una scansione dei processi di sistema ogni 1,5 secondi con un conseguente

intasamento delle risorse di sistema. A questo si aggiunge il fatto che informa il server della Sony ogni qualvolta viene ascoltato un cd protetto, fornendo tutta una serie di informazioni circa il cd che si sta ascoltando, quando e dove.

Alla luce di quanto detto, il DRM adottato da Sony BMG è stato accusato di compromettere la sicurezza di Windows e la stabilità del sistema operativo, di favorire la diffusione di virus e comportarsi da spyware. La Sony BMG con la sua geniale pensata di adottare prodotti anticopia intrusivi e nascosti, non ha certamente fermato la pirateria, nè tanto meno ha incrementato le sue vendite: si è infatti trovata a dover ritornare sui suoi passi mettendo a disposizione di tutti delle apposite procedure di rimozione, dei risarcimenti, e non ultimo, il ritiro dal mercato di milioni di cd protetti.

Nonostante la Sony sostenga che la presenza del rootkit non sia pericolosa e che tutto sia regolare secondo i suoi canoni, una sua prima reazione fu l'annuncio che sul suo sito web sarebbe stata offerta una patch capace di rendere visibile il rootkit, senza disinstallarlo: la XCP.Sony.Rootkit.Patch. L'installazione della richiede però un "iter" piuttosto particolare.

Questa patch risulta essere un vero disastro da quanto confermato da informatici del calibro di Ed Felten e Alex Halderman dell'Università di Princeton: un'analisi dettagliata del software evidenzia una gravissima vulnerabilità di sicurezza che colpirebbe tutti i computer in cui venisse attivato l' uninstaller consigliato da Sony. Felten e Halderman, sostengono che: "*Chi installa la patch consentirà a qualsiasi sito web di scaricare, installare e far girare software sul proprio computer. Qualsiasi pagina web, può prendere possesso del tuo computer e poi farci quello che vuole*".

4.3. Attacchi al sistema Sony BMG

I sistemi DRM adottati per i cd adottano misure anti-copia attive e passive; le misure passive modificano i contenuti presenti sul disco con la speranza di confondere i driver dei computer, senza interessare i player audio dei cd. Le misure di protezione attive

invece, contano su un software presente sul computer che interviene e blocca l'accesso alla musica da parte di programmi diversi dal software proprietario realizzato dal venditore del DRM. I sistemi sono comunque soggetti ad attacchi da parte di utenti che vogliono copiare la musica illegalmente: gli utenti potrebbero infatti sconfiggere la protezione passiva, interrompere l'installazione del software DRM, modificare l'algoritmo di riconoscimento, catturare la musica dal player DRM o disinstallare il software di protezione.

Come già detto in precedenza, quando un disco XCP è inserito in una macchina Windows, l'autorun lancia l'installer XCP. L'installer monitorizza continuamente la lista dei processi in esecuzione sul sistema e confronta l'immagine del nome di ciascun processo con i nomi presenti in una blacklist composta da circa 200 applicazioni. Se verifica che una, o più applicazioni, sono in esecuzione, l'installer sostituisce la finestra dell'EULA con un messaggio di warning, indicando che le applicazioni devono essere chiuse, affinché l'installazione possa continuare con successo.

Inoltre, attiva un timestamp di 30 secondi; se allo scadere dei 30 secondi, tali applicazioni sono ancora in esecuzione, l'installer rilascia il cd ed esce. Questa tecnica dovrebbe prevenire la copia dei dischi, ma essa può essere sconfitta da tecniche ben note. Gli utenti potrebbero uccidere il processo dell'installer (usando il Task Manager), prima che esso rilasci il CD; potrebbero anche usare una applicazione di ripping o copia che blocca la piastra del cd, impedendo il suo rilascio.

Il player XCP è stato progettato per assicurare delle restrizioni d'uso sui contenuti. In realtà esso fornisce un livello di sicurezza minimo: sono stati individuati diversi modi attraverso i quali gli utenti possono abbattere queste limitazioni.
La classe di attacchi più interessante è senza dubbio quella rivolta alla generazione di un numero limitato di copie. E' facile notare come questi sistemi DRM siano vulnerabili ad attacchi di rollback. In un attacco di rollback, lo stato della macchina viene salvato prima che venga eseguita un operazione limitata (in questo caso, un'operazione di copia). Quando l'operazione è completata, il precedente stato del sistema è recuperato e il software DRM non sarà abile a determinare se l'operazione è avvenuta.

Il player XCP usa il file, %windir%\system32\$sys$filesystem\$sys$parking, per ricordare quante copie restano per ogni album XCP che è stato usato sul sistema. Questo file è protetto e nascosto dal rootkit di XCP. Accade però che se il rootkit è disabilitato, un utente potrebbe fare un backup del file, copiare l'album, e poi recuperare lo stato precedentemente salvato, in modo tale che il contatore di copia riporti il valore originale (antecedente alla copia).

CAPITOLO 5: ITUNES STORE & FAIR PLAY

L'iTunes Store (iTunes Music Store fino al 12 settembre 2006) è un negozio on-line per la vendita di musica digitale, video musicali e film gestito dalla Apple Inc. È stato lanciato il 28 aprile 2003 in contemporanea con la versione 4 di iTunes, l'applicazione freeware attraverso cui si ha accesso al negozio.

Figura 22 Screenshot iTunes

Il negozio è supportato dal catalogo delle cinque maggiori case discografiche del pianeta, BMG Music, EMI, Sony Music, Universal e Warner Bros. Esso include anche oltre 300 etichette indipendenti. Offre un repertorio di più di sei milioni di canzoni, incluse tracce esclusive di 20 artisti del calibro di Bob Dylan, U2, Mariah Carey, Sheryl Crow e Sting. Ogni canzone può essere scaricata per 99 US cents. 30 secondi di preascolto sono offerti gratuitamente per ogni canzone. Molti album costano 9,99 dollari statunitensi. È consentito masterizzare un numero infinito di volte le canzoni scaricate.

Il 10 agosto 2004, Apple annuncia che iTunes Music Store ha raggiunto la cifra di un milione di canzoni in catalogo. L'iTunes Store include anche oltre 5.000 audiolibri, codificati a 32 kb/s. Per ogni audio libro sono offerti 90 secondi di preascolto.

Dal 12 ottobre 2005 il negozio vende anche video digitali. Il negozio vende migliaia di video musicali e alcuni programmi televisivi. I programmi vengono immessi nel negozio il giorno dopo la prima trasmissione televisiva. I programmi venduti dal negozio sono principalmente serie televisive trasmesse dalle televisioni via cavo come Friends o Desperate Housewives.

Dal 12 settembre 2006 è possibile acquistare film (per il momento solo negli Stati Uniti) e giochi per iPod; di conseguenza il nome viene modificato in "iTunes Store". Dal 2008 distribuirà film del produttore 20th Century Fox, questi verranno venduti negli Stati Uniti a un prezzo medio di 15 dollari.

Il 15 gennaio 2008 la società ha annunciato la disponibilità di film in affitto. Questi una volta scaricati potranno essere visti entro trenta giorni e una volta iniziata la visione si avrà 24 ore per terminarla. I film a catalogo saranno entro febbraio un migliaio per il nord America. Il costo del servizio è di 3.99 $ per le novità, 2.99 per i film di catalogo. Nel caso si richieda film in alta definizione il prezzo viene maggiorato di un dollaro.

Le canzoni sono codificate nel formato Dolby Advanced Audio Coding [35] a 128 kb/s. Questa codifica ha una qualità equivalente a quella di un file MP3 codificato a 192 kb/s. Dolby Advanced Audio Codec, o AAC, è parte dello standard MPEG-4 contenuto nel

pacchetto multipiattaforma QuickTime 6. Sebbene tecnicamente ogni lettore digitale sia in grado di leggere i file AAC , solo Apple iTunes e iPod possono leggere i file AAC criptati con la tecnologia Apple FairPlay. Recentemente Real Networks ha creato la tecnologia Harmony, per permettere al suo negozio di musica di vendere musica protetta digitalmente ma leggibile dall'iPod. Apple ha minacciato una azione legale contro Real Networks, considerando la tecnologia Harmony una violazione del contratto d'uso legato all'iPod.

Gli altri negozi di musica online utilizzano principalmente la tecnologia proprietaria della Microsoft Windows Media Video, o formato WMV.

5.1. FairPlay

Apple FairPlay è una tecnologia di Digital rights management (DRM) integrata in iTunes, che gestisce le canzoni comprate su iTunes Music Store. Rispetto ad altri sistemi di DRM è meno restrittivo e invasivo. Consente di masterizzare un numero infinito di CD per ogni canzone, copiare le canzoni su un numero illimitato di iPod e di ascoltare le canzoni su un massimo di 5 computer, Mac o PC.

Con l'introduzione di iTunes 4.5, Apple modificò le restrizioni portando il numero massimo di computer utilizzabili per l'ascolto da 3 a 5; modificò inoltre il numero massimo di volte con cui si poteva masterizzare una playlist portandolo a 10 dalle 7 iniziali. Tali modifiche furono consentite dalla rinegoziazione che Apple condusse con le industrie discografiche.

I file protetti con FairPlay sono regolari contenitori MP4 con un flusso audio cifrato AAC [22]. Il flusso audio è cifrato utilizzando l'algoritmo AES in combinazione con la funzione hash MD5. La "master key" è richiesta per cifrare e decifrare il flusso audio ed è anche memorizzata in forma cifrata nel file contenitore MP4. La chiave richiesta per decifrare la master key è detta "user key". Ogni volta un consumatore usa iTunes per comprare una canzone, viene generata in modo casuale una nuova "user key".

Quando un utente autorizza un nuovo computer, iTunes invia un identificatore univoco della macchina ai server Apple. In cambio riceve tutte le user key che sono associate all'account. Questo assicura alla Apple di poter limitare il numero di computer autorizzati e che ogni computer possieda tutte le user key che sono richieste per riprodurre le tracce che l'utente ha acquistato.

Quando un utente de-autorizza un computer, iTunes comunicherà ai server Apple di rimuovere l'identificatore dal loro database, e allo stesso tempo eliminerà tutte le user key dal repository cifrato.

Anche l'iPod dispone di un repository cifrato per le chiavi. Ogni volta che viene copiata una traccia audio protetta con FairPlay, iTunes copierà anche la user key dal suo repository a quello dell'iPod. Questo per assicurare che l'iPod abbia tutto quello che serve per riprodurre il flusso audio AAC.

FairPlay non influenza la capacità di copiare il file, ma solo di decifrare il suo contenuto audio.

5.2. Restrizioni

Alle tracce audio cifrate con FairPlay sono concessi i seguenti permessi:

- La traccia può essere copiata su un qualsiasi numero di lettori iPod.
- La traccia può essere riprodotto su al massimo cinque (in origine tre) computer autorizzati simultaneamente.
- Una particolare playlist all'interno di iTunes contenente una traccia cifrata con FairPlay può essere copiata su un CD al massimo sette volte (in origine dieci) prima di dover cambiare la playlist.
- La traccia può essere copiata su un normale CD audio quante volte si vuole.
    - Il CD audio risultante non ha DRM e può essere rippato, codificato e riprodotto senza limitazioni come un qualsiasi altro CD. Comunque, i CD creati dagli utenti non mantengono i diritti del distributore originale e

non possono essere legalmente noleggiati, prestati, venduti o distribuiti ad altri tranne il creatore del CD stesso.

- Il CD audio contiene ancora gli artefatti derivanti dalla compressione, quindi la conversione a un formato lossy come l'MP3 può aggravare gli artefatti della codifica (vedi transcodifica). Quando si effettua il rip di un CD si può scegliere un codec audio lossless come AIFF, Apple Lossless, FLAC or WAV, che però occupano molto più spazio dei file .m4p originali.

Al momento, le restrizioni menzionate sopra sono codificate all'interno delle applicazioni QuickTime e iTunes, e non sono configurabili all'interno degli stessi file protetti.

Fairplay impedisce ai clienti di iTunes di utilizzare la musica direttamente su un lettore digitale diverso dai seguenti: Apple iPod, Motorola ROKR E1, Motorola SLVR, Motorola RAZR V3i e iPhone.

5.3. Funzionamento di FairPlay

Generalmente la musica che usiamo è codificata nel formato MP3. Questo formato, però, non risulta essere molto utilizzato da parte delle aziende poiché primo di applicazione DRM. A causa di questo motivo, il formato maggiormente usato per questi scopi è l'AAC [22].

AAC è stato sviluppato da alcuni degli stessi esperti che hanno il formato MP3: il Fraunhofer Istitute, Dolby, Sony e AT & T. AAC offre una migliore compressione, il supporto per più canali audio, e richiede meno potenza di elaborazione per la decodifica rispetto ad un file MP3.

ITunes rippa di default i CD usando AAC. La maggior parte dei moderni dispositivi, dei lettori multimediali, telefoni cellulari, riescono a riprodurre file audio AAC. Inoltre

AAC è stato adottato anche per l'uso da parte di Sony per PlayStation Portable e la PlayStation 3, e molti altri lettori di musica al di là degli iPod.

I brani acquistati iTunes Music Store sono protetti con il DRM FairPlay DRM di Apple e codificati con AAC. Senza l'utilizzo delle impostazioni segrete di FairPlay, le altre parti non possono riprodurre i brani.

Al fine di creare un sistema che possa gestire l'accesso a miliardi di brani venduti a milioni di utenti, mantenendo le cose semplici e flessibili, FairPlay utilizza set di chiavi che lavorano insieme per fare in modo che il sistema, anche se viene craccato, mantiene l'impegno di Apple limitando i danni.

Viene presentato ora una descrizione sul funzionamento di FairPlay.

Prima di poter acquistare contenuti da iTunes Store, un utente deve creare un account su Apple.com e successivamente autorizzare un PC o Mac per l'esecuzione di iTunes.

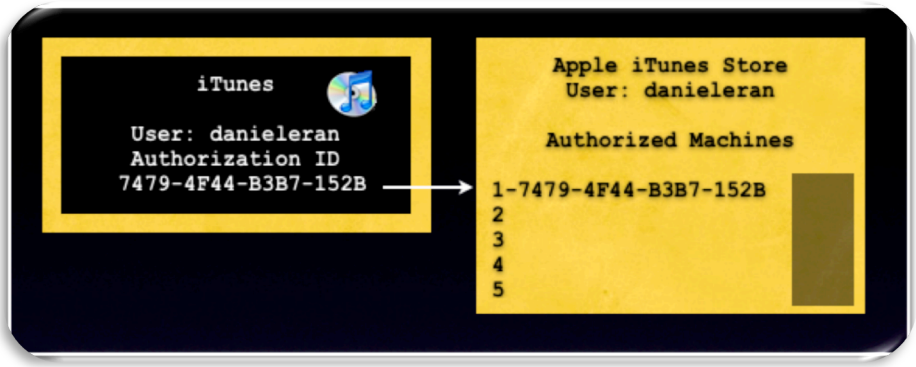

Figura 23 ID del PC dove è in esecuzione iTunes

Durante l'autorizzazione, iTunes crea un numero ID univoco a livello mondiale per il computer dove è in esecuzione, quindi lo invia al server di Apple, dove viene associato all'account di iTunes per un massimo di 5 autorizzazioni per PC differenti.

Il brano AAC viene scaricato da iTunes in chiaro, e al proprio interno ne effettua la cifratura con una chiave master. Viene generato l'hash ed incluso nel file audio protetto. La chiave master viene cifrata con la chiave utente ed inviata ai server Apple.

L'iTunes memorizza quindi sia il contenuto cifrato che il set delle user key e delle master key.

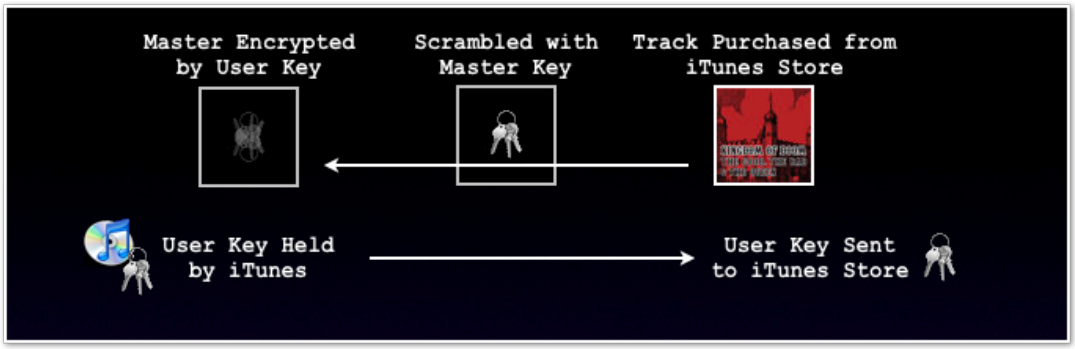

Figura 24 Cifratura del brano audio con la Master Key

Le canzoni vengono mantenute nel server Apple in chiaro e nel momento in cui vengono acquistate, vengono crittografate per funzionare all'interno del "proprio" iTunes. In questo modo, si accelera e semplifica la transazione delegando il lavoro a iTunes sul computer locale. iTunes memorizza queste chiavi sull'hard disk in un database di chiave protetto (un file chiamato SC Info.sidb o noto semplicemente come iTunesDB).

Il risultato è un sistema di autorizzazione che non richiede ad iTunes di verificare ogni canzone con Apple. ITunes mantiene una collezione di chiavi utente per ogni brano acquistato nella sua biblioteca. Per riprodurre un brano protetto AAC, iTunes utilizza la user key per sbloccare la master key memorizzata all'interno della canzone file di canzone e quindi la utilizza per decodificare i dati. Ogni volta che una nuova traccia viene acquistata, una nuova chiave utente deve essere creata, tutte le chiavi sono crittografate e memorizzate sul computer autorizzato da iTunes, oltre ad essere copiate sui server Apple.

Quando si sceglie di utilizzare un nuovo computer, questo deve essere autorizzato. Viene generato quindi un ID univoco e viene inviato ad Apple, che lo inserisce nella

tabella corrispondente all'utente in questione (Apple permette di gestire al massimo 5 PC differenti).

Il server Apple invia al nuovo PC autorizzato l'intero set delle user key per tutti i brani acquistati dall'utente, in modo tale che tutti i sistemi autorizzati saranno in grado di riprodurre tutte le canzoni acquistate.

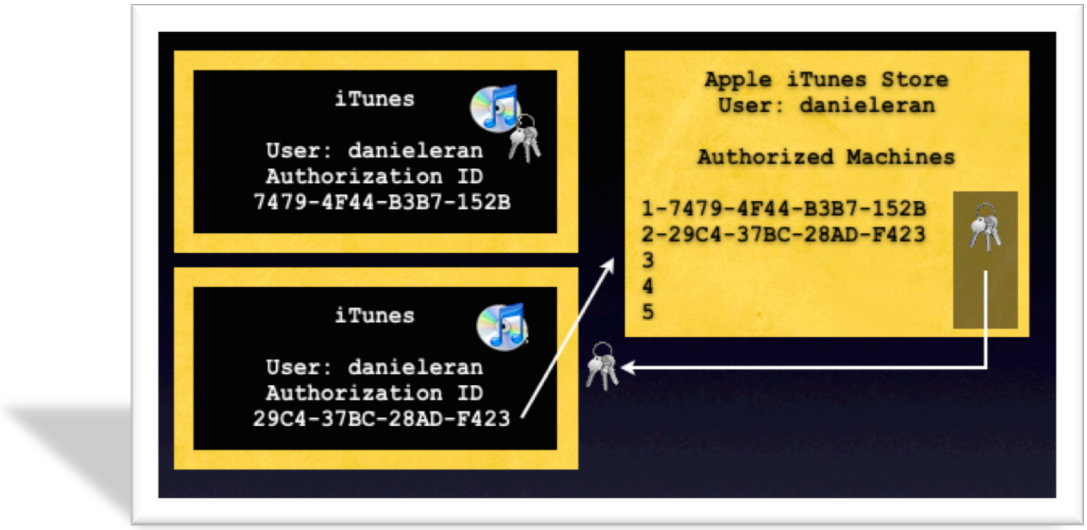

Figura 25 Registrazione di un nuovo PC nell'account Apple

Un computer può essere autorizzato da parte di più utente di iTunes e per ogni account, iTunes memorizza un set di user key.

Quando si decide di eliminare un PC dalla lista dei PC autorizzati, cancella il suo set di chiavi locali e chiede alla Apple di rimuovere l'autorizzazione. Se le chiavi sono state salvate, l'utente può rimuovere l'autorizzazione dai loro sistemi, quindi ripristinare le chiavi e autorizzare un nuovo set di computer, sempre rispettando il limite di 5 PC autorizzati in grado di riprodurre tutti i brani acquistati.

Tuttavia, ogni nuovo brano acquistato su un nuovo PC autorizzato, avrà la corrispettiva user key la quale non può essere riprodotta sul PC precedentemente de-autorizzato poiché quest'ultimo non detiene più le nuove chiavi necessarie per la riproduzione.

5.3.1. Riproduzione di una canzone con DRM su un iPod

Qualsiasi numero di iPod può essere utilizzato con un computer autorizzato che esegue iTunes. Una volta che l'iPod è collegato durante la fase di sincronizzazione con le playlist di iTunes, provvede a scarica tutte le chiavi utente in modo che possa sbloccare e riprodurre qualsiasi brano protetto.

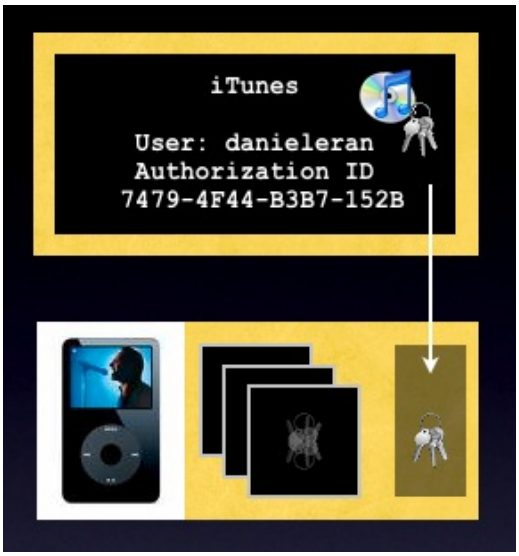

Figura 26 Set di user key trasmesso da iTunes all'iPod

Nel caso in cui iTunes è autorizzato a riprodurre brani per conto di più utenti, tutte le user key di ogni account vengono trasmesso all'iPod. Insomma l'iPod detiene una sorta di database di user key.

L'iPod decide quali brani riprodurre ma semplicemente permette la riproduzione di quelli cui iTunes ha le user key.

Se iTunes ha delle canzoni nella sua libreria ma non possiede le chiavi per riprodurle, semplicemente provvede a non sincronizzarle con l'iPod che verrà connesso. Non c'è modo che brani protetti possono essere copiati sull''iPod senza le user key in quanto iTunes non lo permette.

Questo spiega anche perché gli utenti non possono scambiare la propria musica con quella di un amico in quanto l'iTunes utilizzato per lo scambio, non provvede ad aggiornare il database delle user key. Inoltre un iPod non può sincronizzare più librerie di iTunes in quanto non è in grado di gestirle.

Con iTunes 7 tuttavia, Apple ha aggiunto la capacità ad un iPod registrato di riuscire a sincronizzarsi con qualsiasi computer autorizzato ad un determinato utente. Ogni copia di iTunes può aggiornare le chiavi utente sull'iPod e aggiungere nuovi brani acquistati, assicurando che l'iPod sia in grado di riprodurre tutta la musica sincronizzata.

5.3.2. Come è stato effettuato il Cracking di FairPlay di iTunes

Nel sito ufficiale Apple, nella definizione di FairPlay si legge che "*Dato che i brani sono codificati con AAC protetti, è praticamente impossibile decoficare i brani per essere riprodotti"*. Quello che i cracker fanno è cercare di sottrarre le chiavi in modo che possono decifrare le stesse canzoni nello stesso modo in cui lo fa iTunes.

Come già detto in precedenza, le user key vengono crittografate e memorizzate in iTunes, sull'iPod e sui server Apple. In base all'utilizzo delle chiavi, c'è la possibilità di "rubare" i brani una volta che essi sono stati decodificati. In entrambi i casi, i brani decifrati possono essere recuperati e copiati in un file privo di protezione.

Jon Johansen (conosciuto come DVDJon per il suo coinvolgimento nel cracking del sistema di cifratura dei contenuti DRM utilizzato sui DVD) mentre stava lavorando per costruire un client iTunes per Linux, ha scoperto diversi metodi per eliminare la cifratura sui file protetti da FairPlay:

Figura 27 Jon Johansen

a) Il primo, rilasciato con il nome QTFairUse, non faceva altro che carpire i brani una volta che venivano decifrati da iTunes e memorizzare il flusso dati in un nuovo file AAC privo di protezione.
b) Il secondo, originariamente utilizzato in PyMusique (un client Linux per l'iTunes Store), cerca di imitare iTunes: richiede i brani dai server Apple e successivamente ne effettua il download senza però bloccarli (al contrario invece di come si comporta iTunes).

Queste tecniche funzionano soltanto quando si tratta di una canzone appartenente ad un utente che abbia un account Apple mentre non sono in grado di funzionare con brani acquistati da altri utenti. Infatti il sistema di Fairplay non è stato mai craccato al punto tale da permettere a chiunque di poter riprodurre qualsiasi brano codificato.

5.4. RealNetworks e l'attacco Rhapsody

Il tentativo di Real [26] è quello di vendere la propria musica (comprensiva di DRM) che sia in grado di essere riprodotta anche su un iPod. Poichè il DRM Helix di Real non è in grado di essere riprodotto su un iPod, Real ha realizzato un software in grado di decodificare la propria musica con DRM: esso non fa altro che codificare la musica come se fosse un pacchetto di FairPlay e quindi riproducibile sugli iPod facendo si che il proprio DRM restasse intatto. Apple ha rilasciato una risposta alquanto bizzarra dicendo *"Siamo rimasti scioccati dalla tecnica adottata da RealNetworks per penetrare*

all'interno di un iPod, tecnica paragonabile ad un hacker". Ciò che realmente la Apple ha fatto è stato quello di impedire la riproduzione dei brani Real dalla propria piattaforma.

5.5. La soluzione definitiva di Apple

Il 6 gennaio 2009, Apple, sul proprio sito [24], ha rilasciato una comunicazione riguardante i DRM ed il loro funzionamento con iTunes. Sotto segue l'articolo così come è stato pubblicato.

"***Cambiamenti in arrivo per iTunes Store***

Tutte le canzoni senza DRM

Si potranno scaricare le canzoni direttamente su iPhone 3G attraverso la rete 3G allo stesso prezzo

In Aprile 2009 le canzoni su iTunes saranno disponibili a tre prezzi fissi

SAN FRANCISCO—6 gennaio, 2009—Apple annuncia oggi diversi cambiamenti in iTunes Store (www.itunes.it). A cominciare da oggi, le quattro principali etichette discografiche—Universal Music Group, Sony BMG, Warner Music Group ed EMI, insieme a centinaia di etichette indipendenti, offriranno la loro musica in iTunes Plus, il formato di Apple senza DRM con una più alta qualità di codifica AAC a 256kbs per una definizione audio virtualmente indistinguibile dalla registrazione originale. I clienti di iTunes possono anche scegliere di scaricare le loro canzoni preferite dal più grande catalogo musicale al mondo direttamente su iPhone 3G attraverso la rete 3G così come lo si è fatto attraverso il Wi-Fi sino ad oggi, allo stesso prezzo del download dal computer. Cominciando da aprile, in base a quanto le etichette faranno pagare ad

Apple, le canzoni su iTunes saranno disponibili a tre prezzi differenti: 69 centesimi, 99 centesimi e € 1,29 con la maggior parte degli album ancora al prezzo di € 9,99.

"Siamo eccitati dall'essere in grado di offrire ai clienti di iTunes canzoni iTunes Plus senza DRM in alta qualità audio e ai possessori di iPhone 3G la possibilità di acquistare musica da iTunes in ogni luogo e in ogni momento, attraverso la rete 3G, allo stesso prezzo dell'acquisto con il computer o via rete Wi-Fi, "ha detto Steve Jobs, CEO di Apple. " E in aprile, in base a quanto le case discografiche faranno pagare ad Apple, le canzoni su iTunes saranno disponibili a uno dei tre prezzi stabiliti: 69 centesimi, 99 centesimi e € 1.29, con molte più canzoni al prezzo di 69 centesimi invece di € 1,29"

iTunes offre ai propri clienti una semplice opzione per aggiornare nel formato iTunes Plus l'intera libreria delle canzoni precedentemente acquistate, con una qualità maggiore e senza DRM, per soli 30 centesimi a canzone o al 30 percento del prezzo dell'album. iTunes Store inizierà oggi stesso ad offrire otto dei dieci milioni di canzoni nel formato iTunes Plus senza DRM e gli altri due milioni di canzoni saranno disponibili su iTunes Plus dalla fine di marzo.

Gli utenti di iPhone 3G possono ascoltare l'anteprima e acquistare l'intero catalogo di iTunes attraverso la rete 3G, così come lo fanno oggi attraverso la rete Wi-Fi, allo stesso prezzo e alla stessa qualità. Le canzoni acquistate su iPhone si sincronizzeranno automaticamente con il computer la prima volta in cui sincronizzerà l'iPhone."

CAPITOLO 6: ASPETTI LEGALI

I DRM hanno ricevuto un sostegno giuridico internazionale grazie all'implementazione della Wipo Copyright Treaty (WCT, *Organizzazione Mondiale per la Proprietà Intellettuale*) del 1996. Il WCT è stato effettuato nella maggior parte degli Stati membri del World Intellectual Property Organization. L'implementazione statunitense è la Digital Millennium Copyright Act (DMCA), mentre in Europa il trattato è stato effettuato da una direttiva europea del 2001 sul copyright, che richiede agli Stati membri dell'Unione Europea di effettuare le protezioni legali per le misure preventive tecnologiche.

Le attuali battaglie sui copyright si basano su due questioni:

- ✓ come la legge dovrebbe proteggere i proprietari di copyright;
- ✓ se si può ritenere responsabile per le violazioni di copyright colui che fa un prodotto che può evadere queste misure di controllo.

La pirateria audiovisiva è costituita da qualsiasi sfruttamento illecito di un'opera audiovisiva, che venga effettuato a scopo di lucro da chi non sia titolare dei diritti sulla stessa. I principali settori in cui la pirateria audiovisiva si sviluppa possono essere suddivisi in:

- ✓ pirateria sui titoli di prima visione;
- ✓ mercati e venditori ambulanti;
- ✓ pirateria back-to-back: circuito del noleggio;
- ✓ importazioni parallele;
- ✓ pirateria Via Internet;
- ✓ il diritto alla copia di backup .

Nel 1996, venne formato il **Copy Protection Thecnical Working Group** per esplorare ulteriori tecniche per la protezione dei contenuti dei DVD.

6.1. Italia

La legge italiana sul diritto d'autore (legge 22 aprile 1941 n. 633 [8], in materia di "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio") permette ai titolari di diritti d'autore e di diritti connessi di apporre sulle opere dell'ingegno (brani musicali, film, software, ecc.) misure tecnologiche di protezione efficaci. Esse consistono in tecnologie, dispositivi o componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dal titolare dei diritti. Le "misure tecnologiche di protezione" devono essere rimosse da chi le ha apposte solo in particolari casi stabiliti dalla legge (ad esempio «per fini di sicurezza pubblica o per assicurare il corretto svolgimento di un procedimento amministrativo, parlamentare o giudiziario»).

La legge prevede sanzioni penali nelle ipotesi di elusione dei DRM, come nel caso degli articoli 171-bis (che si applica solo nei casi in cui l'opera dell'ingegno è un "programma per elaboratore") e 171-ter della citata legge 633/41. *"È punito con reclusione e multa chiunque, per trarne profitto, abusivamente importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi o qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un software."* L'art. 171-ter della legge 633/41, poi, punisce penalmente con reclusione e multa chiunque, per uso non personale e a fini di lucro, fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti oppure presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere le misure tecnologiche di protezione; lo stesso accade se le attrezzature, i prodotti o i componenti sono stati principalmente progettati, prodotti, adattati o realizzati per rendere possibile o facilitare l'elusione delle stesse misure. Lo stesso articolo punisce penalmente anche chi abusivamente rimuove o altera le informazioni elettroniche poste sulle opere dell'ingegno. Tali informazioni identificano l'opera protetta e l'autore (o qualsiasi altro titolare dei diritti). L'art. 174-ter della legge 633/41 punisce con la sanzione amministrativa di 154 € (oltre la confisca e

la pubblicazione del provvedimento) chiunque acquista o noleggia attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche.

Appare problematico il rapporto con l'equo compenso: difatti, la presenza di sistemi di DRM, secondo la legge, non può impedire al legittimo possessore di un'opera dell'ingegno di effettuarne una copia privata per uso personale. Pertanto, i titolari dei diritti d'autore devono far sì che ciò sia possibile (articolo 71-sexies, IV comma, della legge 633/41).

Per "indennizzare" i titolari dei diritti d'autore dall'esercizio di tale facoltà, la legge prevede un "equo compenso"; esso consiste in una somma imposta sul prezzo di apparecchiature idonee a registrare contenuti audio o video (masterizzatori, videoregistratori, audioregistratori, periferiche di memorizzazione come schede di memoria, ecc.) e sui relativi supporti vergini. Questo compenso viene incamerato dalla SIAE che poi lo distribuisce ai titolari dei diritti d'autore. La presenza di DRM, però, può rendere virtualmente impossibile effettuare la copia privata.

6.2. Europa

La Direttiva del 2003 afferma che le contraffazioni in Europa dovrebbero fronteggiare le autorizzazioni criminali e multare del doppio del valore di ogni prodotto contraffatto, più i profitti illeciti ottenuti sulla vendita dei prodotti copiati. Questa direttiva deve soltanto essere adottata dai suoi stati membri.

Nel gennaio del 2004, i dirigenti dei più grandi nomi dell’hardware e del software, hanno richiesto all’UE la fine di un antiquato sistema dei tributi sulle copie analogiche.

Il paese che ha dato i natali a DVD Jon, co-autore del famigerato DeCSS e uno degli hacker più esposti nella lotta alle restrizioni da copia, stupisce ancora con quella che appare un'apertura senza precedenti alla libera circolazione dei contenuti digitali online. A farsene carico non è una formazione estrema come il Partito Pirata internazionalista,

bensì il partito politico più vecchio della Norvegia, i liberali di Venstre, che nelle elezioni politiche del 2005 hanno ottenuto il 5,9% dei consensi.

La risoluzione è stata proposta dai Giovani Liberali all'ultimo congresso del partito ed ha ottenuto l'appoggio del vice-presidente in carica Trine Skei Grande. Per quanto, a conti fatti, le proposte parlino della regolamentazione dell'attuale status quo della rete - la circolazione senza freni delle informazioni e dei contenuti digitali - esse rappresentano una presa di posizione inedita all'interno del panorama europeo. Mai fino ad ora si era infatti vista una formazione politica di tale peso e importanza farsi carico di tematiche quali l'abolizione per legge delle tecnologie anticopia o la legalizzazione del file sharing.

"La legge sul diritto d'autore è obsoleta - si legge nella risoluzione - Una società dove la cultura e la conoscenza sono gratuite e accessibili da chiunque in egual misura è un bene comune. I grossi distributori e i possessori dei diritti d'autore abusano sistematicamente e ampiamente del copyright, bloccando quindi lo sviluppo artistico e l'innovazione".

In tal senso, il Partito Liberale si propone di ristabilire l'equilibrio del copyright, così pesantemente squilibrato nei confronti dell'industria e delle associazioni di produttori che fanno un po' il bello e il cattivo tempo, agendo sulle grandi macro-aree individuate nella questione: il file sharing, la campionatura di opere preesistenti, l'estensione temporale del diritto d'autore e il DRM.

L'evoluzione tecnologica, dice il Partito Liberale, ha permesso la diffusione della cultura, sia popolare che di nicchia, in tutto il mondo al minimo costo. Piuttosto che rappresentare una minaccia, questa è una opportunità preziosa da legalizzare, assieme alla concezione di nuove strade per compensare gli artisti e i proprietari del copyright.

Vanno in tal senso riviste le leggi e le regolamentazioni sia norvegesi che internazionali, in modo che esse si occupino di limitare solo l'utilizzo e la distribuzione dei contenuti in ambito commerciale.

Nessun futuro per le tecnologie anticopia, croce e delizia di utenti e major internazionali, che a Venstre vogliono proibire ritenendole limitazioni inaccettabili. La tecnologia di fruizione dei contenuti deve essere neutrale, e i distributori non hanno alcun diritto di controllare l'uso degli audiovisivi legalmente acquistati. Qualora poi l'interdizione di una tecnologia DRM sia al di fuori della giurisdizione norvegese, i produttori dovrebbero essere obbligati a specificare con chiarezza la presenza di restrizioni prima della vendita.

L'incredibile successo globale riscosso dall'iPod e dal negozio di musica virtuale iTunes comincia a impensierire le Autorità di regolazione e le associazioni dei consumatori di diversi Paesi europei che contestano l'incompatibilità del lettore con gli altri player MP3.

In Norvegia, ad esempio, il difensore civico Bjørn Erik Thon ha presentato un esposto sostenendo che i termini di vendita dell'iTunes Music Store – secondo cui i brani scaricati sono compatibili soltanto con l'iPod - violano le leggi nazionali. A supportare le sue tesi anche il Market Council e il Consumer Council, così come i suoi 'colleghi' svedesi e danesi.

6.3. Stati Uniti d'America

La Digital Millennium Copyright Act (DMCA) [9] è un'estensione della legge sul copyright degli Stati Uniti d'America approvata all'unanimità il 14 maggio 1998, che criminalizza la produzione e la diffusione delle tecnologie da parte di utenti che aggirano i metodi tecnici di copia-limitazione, rendendo tutte le forme dei software illegali. Il 22 maggio 2001, l'Unione Europea ha approvato la UE Copyright Directive, un'implementazione della WIPO Copyright Treaty che richiamava la DMCA un'esecuzione del Trattato del copyright del 1996 WIPO che ha richiamato molte delle stesse edizioni del DMCA.

Il DMCA è stato in gran parte inefficace nella protezione dei sistemi di DRM. Tuttavia, la legge è stata usata per limitare la diffusione di tale software inibendo la distribuzione e lo sviluppo, come nel caso di DeCSS.

6.4. Il caso The PirateBay

The Pirate Bay spesso abbreviato TPB e chiamato semplicemente in italiano La Baia, è un sito Internet svedese dedicato all'indicizzazione di file .torrent per la rete BitTorrent. Nasce il 21 novembre 2003 da parte di Gottfrid Svartholm (conosciuto sotto lo pseudonimo di anakata), Fredrik Neij (TiAMO) e Peter Sunde (brokep), affermano attraverso la home page che TPB è "il più vasto tracker di BitTorrent al mondo"[33].

6.4.1. Controversie giudiziarie

Negli Stati Uniti e in diversi altri paesi, le locali giurisdizioni subiscono una sempre crescente pressione da parte delle major cinematografiche e discografiche e da diverse Software House per l'adozione di norme e restrizioni che riducano il fenomeno del file sharing. Negli ultimi anni sono state formulate diverse accuse di violazione dei diritti d'autore contro i responsabili di alcune tecnologie Peer-to-Peer. Esse hanno avuto in alcuni casi pieno successo (come per la causa mossa contro Supernova.org). I governi stanno cercando delle misure efficaci per lottare contro ogni forma di file sharing che però si scontrano con il fatto che, nonostante siano utilizzate per raggiungere lo stesso scopo, tra le diverse tecnologie Peer-to-Peer esistono delle differenze tecniche sostanziali.

I siti torrent, come appunto The Pirate Bay, giustificano la loro possibilità di esistere affermando che non violerebbero alcuna legge, poiché, a differenza di altre tecnologie Peer-to-Peer (come ad esempio eMule, Limewire e Shareaza), i dati da loro ospitati sono solo delle chiavi utili per rintracciare i file condivisi all'interno di migliaia di macchine collegate sulla rete Internet. È su questa distinzione che la difesa di The Pirate

Bay ha basato la sua estraneità alla pirateria, essendo il sito solo un motore di ricerca, un Torrent Finder per l'appunto, come Google, Yahoo o MSN Search. Se si estendesse il reato anche a tali siti, il sistema su cui funziona il World Wide Web potrebbe uscirne fortemente ridimensionato e in parte illegale. La logica della difesa era di fatto ineccepibile, ma l'accusa del caso "MGM Studios, Inc. v. Grokster, Ltd.", venne riformulata sulla base che la detenzione dei suddetti metadata, essendo strettamente legati ai contenuti illegali, incoraggiano di fatto l'infrazione delle leggi sul copyright.

Questi intrighi giuridici sembrano dover ricercare una giustificazione ai numerosi atti punitivi contro i responsabili di siti torrent, tra cui si ricorda il sequestro da parte del governo svedese di tutta la server farm e di tutti i beni personali che sembravano anche lontanamente elettronici del responsabile della compagnia di hosting di The Pirate Bay. Ma questo non scoraggiò i sostenitori del sito. Nonostante l'arresto di alcuni componenti dello staff, alla chiusura del sito seguì infatti una rapida riapertura.

Il 20 agosto 2008, agli amministratori del sito e al ministro della giustizia svedese Beatrice Ask, è stata recapitata una nota da parte del Comitato Olimpico Internazionale in cui si affermava che la cerimonia di apertura era scaricabile tramite Pirate Bay; si chiedeva quindi la collaborazione del ministro per la rimozione di tutti i file inerenti la cerimonia. Il ministro ha anche affermato che Pirate Bay getta cattiva luce sulla reputazione della Svezia.

Tra le varie società che hanno aperto controversie giudiziarie contro The Pirate Bay per la violazione del copyright, si segnalano:

- Microsoft;
- Apple;
- Dreamworks;
- EA Games;
- Sublimal Sounds;
- Uppsala universitet;
- ADV Films;
- SEGA;

- White Stripes;
- Warner Bros;
- iRacing;
- Linotype;
- Governo svedese;
- Governo italiano.

Il 17 Aprile 2009 i quattro responsabili di Pirate Bay sono stati condannati a un anno di prigione per complicità nella violazione di diritti d'autore. Lo ha reso noto un tribunale di Stoccolma. "Il tribunale di Stoccolma ha oggi condannato le quattro persone che erano processate per complicità in violazione della legge sul diritto d'autore. Il tribunale ha deciso di condannare ciascuno di loro ad un anno di carcere", precisa la corte in un comunicato. Il tribunale ha condannato Fredrik Neij, 30 anni, Gottfrid Svartholm, 24 anni e Peter Sunde, 30 anni, fondatori di Pirate Bay, e Carl Lundstrm, 48 anni, accusato di avere investito nel sito. I quattro dovranno anche versare 30 milioni di corone (2,7 milioni di euro) di danni e interessi all'industria discografica, cinematografica e dei videogiochi, che reclamavano 117 milioni di corone a titolo di mancati guadagni. La condanna è conforme alle richieste del procuratore che aveva pronunciato la sua requisitoria il 2 marzo. Il processo, durato tre settimane, è considerato come uno dei più importanti contro la pirateria informatica. I legali dei quattro hanno immediatamente annunciato di voler ricorrere in appello. Pochi giorni dopo la sentenza, l'emittente radiofonica Sveriges Radio ha rivelato che il giudice Tomas Norström è affiliato a diverse associazioni pro-copyright, tra cui una a cui appartengono i legali dei titolari di copyright che erano parte attrice nel processo contro The Pirate Bay. E'probabile perciò che più che a un appello si giunga a un nuovo processo.

6.4.2. In Italia

L'indagine condotta dalla Procura della Repubblica di Bergamo e l'adeguamento da parte dei provider al provvedimento emanato dal Giudice per le Indagini Preliminari hanno scatenato non poche polemiche: gli utenti della rete italiani temono dirottamenti

da parte dei provider e incursioni alla privacy da parte dell'industria dei contenuti; provider e industria dei contenuti assicurano di non aver avuto alcuna intenzione di procedere all'arrembaggio dei dati degli utenti. I provider italiani avrebbero dovuto inibire agli utenti italiani l'accesso al motore di ricerca di file condivisi deviando il traffico a mezzo DNS e rendendo inaccessibili tutte le manifestazioni online presenti e future della Baia dei Pirati. Nel giro di una manciata di giorni il provvedimento è stato messo in atto: per evitare che i cittadini della rete approfittassero di link che possono agevolarli nel download di materiale eventualmente protetto dal diritto d'autore, le URL che corrispondono all'IP della Baia hanno iniziato a condurre gli utenti verso pagine vuote o occupate dalle segnalazioni del blocco.

Una volta venuta a galla, la questione ha scatenato l'apprensione di molti: redirezionare il traffico verso un sito gestito da privati avrebbe potuto consentire ai gestori di ProMusic di raccogliere informazioni relative agli utenti di The Pirate Bay. Si sarebbero potuti raccogliere indirizzi IP che rappresentano utenti che accedono alla Baia con gli intenti più diversi, si sarebbe potuto frugare fra le informazioni veicolate dai cookie, si sarebbe potuto agire a nome degli utenti. Non si tratta che di ricostruzioni di scenari potenziali, ricostruzioni che hanno scatenato le apprensioni e le mobilitazioni dei cittadini della rete.

6.4.3. Considerazioni

Il verdetto di colpevolezza che il Tribunale di Stoccolma ha emanato nel mese di aprile contro il gruppo di The Pirate Bay (che ricorrerà in appello) è certamente il primo step giuridico di una vicenda che probabilmente passerà alla Storia. Perché il mondo del copyright è prossimo ad una svolta e questo caso la rende sempre più necessaria.

La svolta deve avvenire nel settore delle regole del mercato. Un mercato in cui esistono grandi aziende, le cosiddette major, detentrici dei poteri forti, che vedono Internet come un pericolo: la Rete consente una democratica distribuzione del sapere e della proprietà intellettuale, rappresentando un’alternativa più efficace ed efficiente dei tradizionali

canali di distribuzione utilizzati da chi produce contenuti. È pur vero che la Rete, proprio per questo, consente anche più facilmente di violare il copyright e ciò è possibile dal momento in cui i contenuti distribuiti sono stati smaterializzati.

Basti pensare alla musica: non più costretta al legame che nel secolo scorso ha sempre avuto con un supporto fonografico, oggi può essere distribuita su Internet come un qualunque file e può essere riprodotta con la medesima qualità del file originale. Ovviamente la pirateria ha vita più facile, perché non è costretta a limitare il proprio commercio a supporti duplicati, ma può raggiungere i propri clienti dalla Rete. Per questo motivo le major tentano di correre ai ripari e si rivolgono alle Istituzioni affinché la tutela del copyright venga estesa ad Internet e puntano il dito contro i provider e contro chi offre piattaforme di content-sharing.

La svolta deve avvenire sul fronte delle regole del mercato e nei modelli di business seguiti dalle aziende che distribuiscono contenuti. Le major ancora non vogliono e non riescono a vedere oltre a ciò a cui sono abituate, ma esistono molte realtà che mostrano come il cambiamento in atto in questo settore sia importante: fra queste c'è ad esempio Jamendo, una community basata su una piattaforma di raccolta e distribuzione di musica libera pubblicata con licenze Creative Commons o con la Licenza Arte Libera che può essere scaricata liberamente senza alcun problema legale.

Esistono inoltre etichette indipendenti come Magnatune, che stipula contratti con gli artisti e trasferisce loro la metà di ciò che guadagna dalla vendita di musica: l'aspetto innovativo è che è l'acquirente a decidere il prezzo di acquisto (non esiste il concetto di listino). Inoltre, prima di decidere l'acquisto stesso, l'acquirente può ascoltare gratuitamente in streaming un brano in formato MP3. Questo stesso tipo di filosofia è stato seguito anche da band come i Radiohead, che dall'uscita dell'album In rainbows (ottobre 2007) si sono resi autonomi nella distribuzione delle proprie opere e si sono permessi di chiudere le porte in faccia ad iTunes di Apple, procedendo alla vendita direttamente dal proprio sito e al prezzo deciso dagli acquirenti.

E' importante che si trovi il punto di incontro tra diritti e interessi degli artisti e quelli degli utenti-consumatori. Non è possibile che le major tentino di cambiare la natura di

Internet in nome del copyright e, alla luce di questa realtà in cambiamento, appare già anacronistico il commento della Fimi (Federazione Industria Musicale Italiana) che, sottolineando il fatto che The Pirate Bay è oggetto di indagine anche in Italia, osserva per bocca del presidente Enzo Mazza: "Il tribunale di Stoccolma sembra aver accolto in pieno le prove, tra le quali anche i dati sui danni provocati da Pirate Bay a produttori ed artisti italiani, dando un efficace segnale che l'illegalità non è tollerata".

CONCLUSIONI

Analizzando questo lavoro, possiamo facilmente dedurre che attualmente non vi sono efficaci DRM, resistenti da attacchi, che impediscono la copia o che limitino la riproduzione.

Per questo motivo, le major vorrebbero che venissero bandite per legge tutte le apparecchiature audio e video, a favore delle uscite digitali con funzioni di DRM e di crittazione dei segnali in uscita dai riproduttori, limitando gli acquirenti oltreché nella copia, anche le possibilità di riproduzione dei file musicali. Attualmente, questo tipo di connettori garantiscono l'interoperabilità fra le apparecchiature audio, permettendo di collegare ad esempio le cuffie al proprio computer, le casse amplificatrici o il proprio lettore MP3 al jack dell'autoradio.

Richard M. Stallman, informatico di fama mondiale, ha voluto sottolineare l'invasività di molte tecnologie DRM (si veda, come esempio, il rootkit utilizzato da Sony in diverse sue produzioni) reinterpretando l'acronimo come "Digital Restrictions Management" (letteralmente "gestione delle restrizioni digitali").

Universal e Virgin sono le due uniche major che vendono brani anche in formato MP3, privo di DRM.

Oggi i file protetti dai DRM non sono tantissimi, la maggior parte delle persone estrae gli mp3 dai CD o scarica i file musicali dalla rete attraverso il P2P, in buona sostanza sono poche le persone che si ritrovano a maneggiare file protetti, quei pochi che lo fanno utilizzano piattaforme software ed hardware integrate e molto recenti, che ovviamente non presentano alcun problema di interoperabilità.

Ad esempio, moltissime persone utilizzano l'iPod per ascoltare musica protetta dai DRM scaricata da iTunes music store.

I DRM non fanno altro che aggiungere un ulteriore strato di complicazione verso l'interoperabilità tra periferiche e sistemi operativi, e tra sistemi operativi diversi.

Se consideriamo il DRM come un software, e precisamente come dei software chiusi, basati su standard chiusi, allora possiamo facilmente comprendere quanto sia plausibile aspettarsi che, tra qualche anno, tutti i file basati su un particolare DRM non saranno più utilizzabili dall'utente che li possiede.

Cercare di aprire un file protetto con un DRM "obsoleto", equivarrebbe, in parole povere, a cercare di infilare un mouse USB in una porta PS2.

Ci possiamo immaginare in caso in cui un domani l'iPod fosse rimpiazzato da un iPod Ver2, e nel frattempo iTunes si fosse anch'esso evoluto, implementando un sistema DRM più efficace e diverso da quello attuale, gli utenti si ritroverebbero con un sacco di file mp3 protetti con il DRM versione 1, che funzionano solo sull'iPod1, e che quindi sono completamente da buttare.

Se quei file fossero stati dei semplici MP3 non protetti da DRM, sarebbe stato ancora possibile ascoltare tali file con un qualsiasi software o lettore mp3 in commercio, ma l'implementazione del DRM rende tutto ciò impossibile, ed all'utente finale non rimane che buttare via tutti i suoi mp3 regolarmente acquistati o sperare che qualcuno sia così clemente da implementare un'utility per convertire i file in un formato nuovamente usabile.

Chi difende le libertà civili sostiene che l'uso della tecnologia digitale dovrebbe essere libero a discrezione del consumatore che ha acquistato quella canzone o quel film e che il passaggio di tale controllo ai produttori anche dopo la vendita produrrà danni sia alla creatività che ai diritti dei consumatori. La maggior parte dei contenuti multimediali oggi (CD musicali, DVD) è protetta da qualche forma di DRM ma al consumatore, che ha acquistato regolarmente il prodotto, dovrebbe essere garantito il diritto alla copia privata ad esempio per realizzare copie di backup. Tutte le tecnologie DRM esistenti attualmente non sono in grado di garantire tale diritto del consumatore e per questo sono in molti a sostenere che il DRM limita l'uso legale del contenuto protetto.

Sotto verranno elencate una serie di problematica che sono state introdotte dai DRM e dalla loro politica.

Dal punto di chi produce i contenuti, i DRM non convengono perché:

1. il DRM non è in grado di impedire l'uso illegale dei file, rende solo più difficile accedervi ed utilizzarli. Molti editori hanno l 'impressione che una volta inserite protezioni DRM su un file non ci siano conseguenze. Pensano: "male non può fare". Invece si sbagliano. Ci sono moltissimi strumenti per rimuovere facilmente tali protezioni dai file. Per cui nonostante il DRM abbia reso la condivisione illegale un po' più difficile (per alcuni soggetti) se qualcuno vuole davvero procurarsi una versione non protetta del file, nel breve tempo riesce a procurarsi facilmente una copia pirata;
2. è sufficiente che anche una sola persona riesca a trovare il modo per violare la protezione di un file e lo renderà disponibile a tutti. Sulle reti Peer-to-Peer è sufficiente anche una sola copia non protetta di un file per metterla a disposizione del mondo intero. Utilizzando il motore di ricerca di qualsiasi programma p2p è facile accorgersi come ci siano in giro canzoni che si suppone possano essere vendute solo online (nella loro versione digitale) inserite in file protetti da DRM;
3. chi vende contenuti su CD sta già vendendo qualcosa di non protetto. Con l'eccezione del rootkit Sony, cui il suo comportamento è stato discusso nel capitolo 4, il 99% dei CD in vendita contiene file non protetti. Questo significa che chi vende contenuti su CD rende disponibile contenuti non protetti e che rendere disponibili quei file online è tanto semplice quanto rippare un CD audio e ricavare i relativi file mp3, operazione banale con i software disponibili oggigiorno. Quello che non si riesce a capire è come mai le aziende discografiche ed i produttori da una parte vendano CD con contenuti non protetti e dall'altra insistano ad inserire protezioni alla copia per i file digitali scaricabili;
4. il DRM costa ai produttori di contenuti. Implementare schermi DRM non è un'operazione gratuita. I costi per sviluppare e/o acquistare licenze DRM, codificare i file multimediali ed affrontare le lamentele dei consumatori confusi da funzionamenti strani dei file appena acquistati vengono trasferiti dai distributori ai produttori. Questo significa che chi produce contenuti fa meno

soldi vendendo contenuti protetti da DRM piuttosto che vendendo contenuti liberi da protezioni;

5. c'è un grande costo nascosto per chi vuole vendere contenuti con DRM. Oltre agli ingenti costi per implementare i DRM, c'è un costo che viene spesso trascurato: quello derivato dalle mancate vendite perché nella maggiore dei casi, la gente non vuole comprare contenuti con DRM o semplicemente perché possiede lettori incompatibili con i file venduti. Inoltre poiché non esiste uno standard di protezioni DRM compatibile universalmente con ogni dispositivo, molta gente non è nelle condizioni di acquistare quel contenuto semplicemente perché non possiede un player compatibile.

Gli aspetti negativi che, invece, coinvolgono i consumatori sono:

1. spesso i costi del DRM gravano anche sulle spalle dei consumatori. Poiché, come abbiamo detto, il DRM non è una tecnologia gratuita, qualcuno dovrà pagarla. Prediamo l'esempio di eMusic ed iTunes. Su iTunes le canzoni costano 99 centesimi mentre su eMusic 25. Una delle ragioni per cui eMusic può vendere musica ad un prezzo tanto inferiore è perché non spende tonnellate di denaro per implementare sistemi DRM e risolvere i problemi dei consumatori con la musica acquistata. E' possibile quindi offrire un prodotto tecnicamente superiore ad un prezzo molto inferiore;
2. il contenuto privo di DRM potrà essere riprodotto su un dispositivo di oggi e di domani. Molti resteranno sicuramente shokkati quando, acquistato un prodotto da una casa costruttrice e consta che i brani acquistati altrove con DRM non sono riproducibili sul nuovo dispositivo;
3. i nostri dispositivi del futuro saranno sicuramente e decisamente diversi dai dispositivi multimediali del presente. In quel caso ogni contenuto con DRM che acquistiamo oggi probabilmente non potrà più essere fruito. Ogni giorno vengono venduti milioni di cellulari capaci di riprodurre mp3, pochissimi sono capaci di riprodurre canzoni di iTunes. Per cui se siamo fondamentalmente interessati a poter usare quello che acquistiamo (considerando che i soldi non

crescono sugli alberi) dovremo pensarci due volte prima di acquistare qualcosa infettato da protezioni DRM;

4. il DRM sposta il controllo sui brani che vengono creati dall'inventore verso altri;
5. acquistando contenuti con DRM si supporta il sistema dei DRM. Acquistando ogni singolo file protetto da DRM contribuiamo a perpetuare un sistema nel quale si considera giusto usare protezioni DRM. Allo stesso tempo frequentando siti e store con contenuti senza DRM, scaricando dalle reti peer-to-peer contenuti con licenze copyleft [25], aiutiamo a rafforzare un sistema nel quale il DRM è considerato inaccettabile ed un modo poco giusto di fare affari.

Il problema della "protezione di copia" diviene sempre più un problema difficile a cui porre rimedio e la motivazione risiede sostanzialmente nel fatto che la tecnologia cd sia una tecnologia di vecchia data ma, soprattutto, ampiamente studiata.

Ricerche future dovranno pertanto mirare ad uno standard unico su cui iniziare a lavorare per raggiungere un elevato livello di sicurezza da applicare ad ogni tipo di contenuto digitale. Nessuno infatti, al giorno d'oggi, è ancora in grado di dichiarare di possedere una tecnologia "a prova di pirateria".

Una efficace strategia del DRM dovrà dunque basarsi su tecnologie difensive, non offensive dunque, che riconoscano la costante necessità di:

- comprendere i mercati;
- conoscere le forze antagoniste;
- calcolare i rischi della loro azione.

Spesso e volentieri le cose sembrano funzionare correttamente, ma questo solo fino a quando una delle variabili in gioco (aggiornamento del DRM, cambio marca del player che non riesce a decodificare il DRM, ecc) non cambia, a quel punto si cominciano a sperimentare spiacevoli e sgradite sorprese.

La coesistenza di equo compenso e di sistemi di DRM è inaccettabile dal punto di vista giuridico, perché la presenza dell'equo compenso dovrebbe rendere illeciti tali sistemi:

di fatto si costringe un soggetto a pagare sempre e comunque senza mai avere una contropartita adeguata (ad es., per avere una copia su audiocassetta di un cd audio legittimamente acquistato) o senza averla affatto (quando non è possibile effettuare la copia)!

Il problema principale è che l'impianto normativo italiano è chiaramente vecchio ed inadeguato, come del resto sostenuto da gran parte dei giuristi italiani. Ancor più grave è, però, il fatto che la l. 633/41 sia squilibrata nel tutelare i titolari dei diritti d'autore a scapito dei legittimi possessori; non sembra che nel prossimo futuro sarà possibile registrare un'inversione di tendenza (basti pensare alla già celebre direttiva IPRED2). Come si è detto, nella fase di applicazione del diritto c'è poco da fare: bisogna fare i conti con la legge scritta e, dunque, gli utenti hanno a disposizione pochi mezzi giuridici per contrastare le pretese delle loro "controparti".

Si dovrebbe comunque fare in modo che il contenuto possa essere più facilmente acquistato che rubato.

BIBLIOGRAFIA

[1] Wikipedia, http://it.wikipedia.org/wiki/Digital_rights_management, ultimo accesso 28-04-2009

[2] MLS LaserLock International, http://www.laserlock.com/, ultimo accesso 07-05-2009

[3] Macrovision Corporation, http://www.macrovision.com/company.htm, ultimo accesso 12-06-2009

[4] Sony DADC, http://www.securom.com/solution.asp, ultimo accesso 28-03-2009

[5] Cd-Cops, http://www.linkdata.com/cdnetman.htm, ultimo accesso 07-05-2009

[6] iTunes, http://www.apple.com/it/itunes/whatis/, ultimo accesso 20-04-2009

[7] CMCC, http://www.musiccreators.ca/wp/, ultimo accesso 28-03-2009

[8] Legge 22 aprile 1941, n° 633, http://www.webstartsrl.it/wspro/demo/files/leggedirittoautore.pdf, ultimo accesso 12-06-2009

[9] Digital Millennium Copyright Act, http://www.copyright.gov/legislation/dmca.pdf, ultimo accesso 28-03-2009

[10] DVD Forum, http://www.dvdforum.org/forum.shtml, ultimo accesso 28-03-2009

[11] DVD: Caratteristiche e protezione, http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0203/dvd/protezione_dvd.htm, *"Avagliano Giuseppe, Catalano Pietro, De Martino Paola, Lima Annalisa"*, ultimo accesso 28-04-2009

[12] 4C Entity, http://www.4centity.com/, ultimo accesso 29-03-2009

[13] Dream Stream , http://dreamstream.info/index.php?option=com_content&task=view&id=23&Itemid=9, ultimo accesso 03-05-2009

[14] Digital Watermarking, http://www.ing.unisannio.it/donofrio/watermarking.php, *"Ing. Salvatore D'Onofrio, Università degli Studi del Sannio, Research Centre on Software Technology (RCOST)"*, ultimo accesso 29-03-2009

[15] DVD Copy Control Association, Content Scramble System (CSS). http://www.dvdcca.org/css/, ultimo accesso 01-04-2009

[16] 4C Entity, LLC. C2 Block Cipher Specification Revision 1.0, January 1, 2003, http://www.4centity.com/docs/versions.html, ultimo accesso 01-04-2009

[17] Wikipedia. Cifrario di Feistel, http://it.wikipedia.org/wiki/Cifrario_di_Feistel, ultimo accesso 07-05-2009

[18] Blog tecnico di Mark Russinovich. http://www.sysinternals.com/blog, ultimo accesso 01-04-2009

[19] Serial Copy Management System. http://en.wikipedia.org/wiki/Serial_Copy_Management_System, accesso 01-04-2009

[20] *"Nuove tecniche DRM per la protezione di copia"*, Lucarelli Maria Annunziata

[21] How to work FairPlay, http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html, ultimo accesso 26-04-2009

[22] AAC, http://it.wikipedia.org/wiki/Advanced_Audio_Coding, ultimo accesso 03-05-2009

[23] VLC media player, http://www.videolan.org/vlc/features.html, ultimo accesso 03-04-2009

[24] La soluzione definitiva di Apple, http://www.apple.com/it/pr/comunicati/2009/01/06-itunes.html, ultimo accesso 07-05-2009

[25] CopyLeft, http://it.wikipedia.org/wiki/Copyleft, ultimo accesso 30-04-2009

[26] Rhapsody, http://service.real.com/rhapsody/, ultimo accesso 03-04-2009

[27] Il DRM in Europa, http://punto-informatico.it/1959066/PI/News/drm-oggi-rischia-europa.aspx, ultimo accesso 03-04-2009

[28] How to work CPRM, http://www.4centity.com/docs/How_CPRM_Works.pdf, ultimo accesso 12-06-2009

[29] ISO 8372, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=15530, ultimo accesso 01-05-2009

[30] Funzionamento CPRM, http://www.intel.com/technology/itj/2002/volume06issue04/art05_protection/vol6iss4_art05.pdf, ultimo accesso 03-05-2009

[31] Funzionamento di AACS, http://www.aacsla.com/specifications/specs091/AACS_Spec_Prerecorded_0.91.pdf, ultimo accesso 12-06-2009

[32] Componenti di AACS, http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf, ultimo accesso 07-05-2009

[33] The PirateBay, http://thepiratebay.org/, ultimo accesso 10-05-2009

[34] HDCP, http://en.wikipedia.org/wiki/High-bandwidth_Digital_Content_Protection, ultimo accesso 06-07-2009

[35] Dolby Advanced Audio Coding, http://www.dolby.com/consumer/technology/aac.html, ultimo accesso 08-07-2009