

DRM, Vista i els vostres drets

Borys Musielak

Traducció[†] al català: Orestes Mas Casals

23 de gener de 2007

Resum

Als EUA, França i alguns altres països ja és prohibit de reproduir música o vídeos adquirits legalment utilitzant reproductors multimèdia de GNU/Linux. Us sona a ciència ficció? Malauradament no ho és. I la cosa no s'acaba a l'esfera multimèdia. Benvingut a la nova era del DRM¹!

Índex

1 DRM, computació confiable...	2
2 DRM exemple a exemple	3
3 El preu del DRM o... què diu Gutmann	4
4 DRM i la llibertat, o què diu Richard Stallman i la FSF	6
5 Què és tot això i com podeu protegir-vos	7
6 Trencar la DRM – és... senzill	8
7 Si però, és legal?	8
8 Més informació sobre la DRM	9

*

⁰ Article original a <http://polishlinux.org/gnu/drm-vista-and-your-rights/>

¹ DRM són les sigles angleses de “Digital Rights Management”, que en català significa “Gestió Digital de Drets”. Els opositors a aquesta mena de tecnologia l’han rebatejada amb el nom anglès de “Digital Restrictions Management”, o “Gestió Digital de Restriccions”, perquè adueixen que descriu millor la seva funció. Sigui com sigui, en aquest document no hem traduït les sigles angleses perquè són més conegudes que les catalanes i permeten aquesta doble interpretació. (N. del T.)

En aquest article m'agradaria explicar el problema de la Gestió Digital de Drets (o Restriccions), especialment en la versió que promou Microsoft amb el nou llançament de Windows Vista. No tothom està familiaritzat amb els perills del nou "estàndard" per tota la indústria informàtica. Si, *tota la indústria*, atès que va molt més enllà del programari produït pel gegant de Redmond i els seus afiliats.

1 DRM, computació confiable – quina mena de bèstia és això?

Citant la Viquipèdia²:

La Gestió Digital de Drets és un terme que aplega les diverses tecnologies orientades utilitzades pels editors o propietaris dels drets d'autor per tal de controlar l'accés i l'ús de dades i maquinari digitals, i les restriccions associades a una còpia concreta d'obra o dispositiu en format digital. El terme es confón sovint amb la protecció contra còpia i les mesures tecnològiques de protecció; aquests dos termes fan referència a tecnologies que controlen o restringeixen l'ús i l'accés a contingut digital en els dispositius electrònics que les incorporen, actuant com a components d'un disseny DRM.

Un terme semblant al DRM (però més especialitzat) és la *computació confiable*³. Aquest terme és intencionadament confús atès que no pretén millorar la seguretat de l'usuari, sinó que pretén assegurar que l'usuari sigui "de confiança". Òbviament, no és una qüestió de confiança, sinó de diners. Les companyies que ofereixen continguts (especialment de tipus multimèdia, però no restringit exclusivament a aquests) al client volen ser capaces de controlar la manera en què aquests continguts s'utilitzen. Per exemple, volen que el contingut només pugui ser reproduït a través de mitjans aprovats, descartant totes les aplicacions "il·legals" (aquí el mot "il·legal" no significa que violi la llei sinó l'acord entre el client i la companyia que ven el mitjà). Podeu trobar més informació sobre la *computació confiable*⁴ a la Viquipèdia.

Però, què té de dolent aquesta pràctica? Per quin motiu les companyies no haurien de poder controlar els seus continguts? La idea del DRM presenta dos aspectes que són importants (i potencialment perillosos) pels usuaris d'ordinadors. El primer aspecte és tecnològic, i el segon, ètic. Tot seguit tractem ambdós.

Ras i curt, l'aspecte tecnològic del DRM implica que el programari o -encara pitjor- el maquinari s'ha de fabricar no pas per poder oferir les prestacions i estabilitat més elevades, sinó per atènyer la millor protecció possible dels drets d'autor. Això presuposa que nosaltres -els usuaris- pagarem més diners per un producte defectuós (ja que no permet certes funcionalitats per raons no tècniques) i ofereix unes prestacions inferiors.

L'aspecte ètic és encara més perillós. En el món del DRM succeeix que no podem fer allò que volem amb els productes que hem adquirit legalment (com ara programes,

²No la catalana, sinó la traducció de l'anglesa (N. del T.)

³"Trusted Computing", en anglès. (N. del T.)

⁴http://en.wikipedia.org/wiki/Trusted_computing/

música, vídeos o documents de text). Allò que podem fer i allò que no ho decideix el proveïdor, no pas nosaltres. Per exemple, un producte protegit per DRM pot ser desactivat en qualsevol moment pel proveïdor si ell creu que estem violant els termes de l'acord. Això significa que la vostra col·lecció de música “protegida” pot ser inutilitzada (rebaixant-ne la qualitat o fins i tot esborrant-ne el contingut) en qüestió de segons, sense el vostre consentiment. És aquesta per ventura alguna horrible visió d'algun dictador maligne i malalt? Doncs no. És la terrorífica era del DRM que s'acosta.

2 DRM exemple a exemple

Així doncs, quin aspecte té el DRM? El podem veure o està amagat? De fet, força companyies famoses han decidit que el DRM és el camí a seguir. Al dessor presentem una llista dels formats més populars que estan afectats (tacats) per la “protecció de drets”:

- ➔ **DVD** - el disc en si no conté cap maquinari DRM, però molts proveïdors van decidir emprar les restriccions recomanades per l'organització **DVD CCA**⁵, com ara el **CSS**⁶ (codificació de continguts utilitzant mecanismes de xifrat) o els **RPC**⁷ (codis regionals).
- ➔ **HD DVD** - malauradament, el nou estàndard que probablement reemplaçarà el DVD ha estat contaminat pel DRM des de la seva creació. La principal restricció que s'utilitza és l'**AACS**⁸, una versió moderna del CSS.
- ➔ **AAC** - és un format de fitxer d'àudio inventat i promogut per Apple i la seva botiga de música iTunes. A la versió amb el sistema de protecció **FairPlay**⁹ (sic!) hi ha restriccions de tipus DRM (xifrat) destinades a impossibilitar la reproducció d'aquest format per part dels reproductors de la competència (les obres xifrades amb AAC només funcionen correctament en productes Apple com ara iTunes, iPod i pocs altres reproductors aprovats per Apple)
- ➔ **Windows Media** - cadascun dels formats del paquet Windows Media (WMV, WMA, WMP o ASF) ha estat contaminat **amb algun tipus de DRM**¹⁰, cosa que acostuma a significar que el contingut està protegit amb tècniques de xifrat simètric i, si les claus no són accessibles, l'usuari només pot veure/escollar una versió degradada del contingut (molt baixa qualitat).

El que és més interessant i no gaire conegut és que el DRM no està restringit als multimèdia. Es pot emprar per protegir qualsevol altre “bé digital”, especialment el programari. La idea de restringir l'accés al programari privatiu mitjançant tecnologies DRM en el maquinari està guanyant popularitat entre els principals proveïdors de

⁵<http://en.wikipedia.org/wiki/DVD.CCA>

⁶http://en.wikipedia.org/wiki/Content_Scramble_System

⁷http://en.wikipedia.org/wiki/Regional_lockout

⁸http://en.wikipedia.org/wiki/Advanced_Access_Content_System

⁹<http://en.wikipedia.org/wiki/FairPlay>

¹⁰http://en.wikipedia.org/wiki/Windows_Media_DRM



Figura 1: Capsa per a l'iPod dissenyada per Jeremy Clark

programari, com ara Microsoft i Apple. Si això es duu a la pràctica, els creadors del programa podran, per exemple, impedir la utilització de certs programes si creuen que són perillosos o il·legals. Això pot voler dir bloquejar programes de la competència si aquests violen les regles internes de l'empresa (p.ex., permeten que l'usuari pugui reproduir DVD o fitxers AAC xifrats, malgrat que no sigui il·legal fer-ho al país de l'usuari). Una altra opció podria ser blocar els clients *peer-to-peer*, com ara eMule o Gnutella (sense importar si s'utilitzen legalment o no). I hi ha moltes altres opcions disponibles, en cas que el DRM sigui acceptat pel gran públic...

3 El preu del DRM o... què diu Gutmann

Peter Gutmann¹¹ ha analitzat en una publicació recent el **cost de la protecció de continguts al Windows Vista**¹² [versió en PDF¹³ de Max Moritz Sievers], fent un èmfasi especial en els doblers reals que haurà de desembutxacar l'usuari de l'ordinador si els fabricants de maquinari implementen aquestes recomanacions. L'article és interessant, però llarg i molt tècnic, per la qual cosa he decidit resumir-ne aquí els punts més importants. Si preferiu llegir l'article original, us encoratgem a fer-ho. Altrament podeu llegir el nostre resum, per tal que sapigau de què estem parlant.

Així doncs, què succeirà si la visió de Microsoft es fa realitat?

- Si heu adquirit recentment una tarja de so d'alta gama potser quedareu sorprès, ja que no podreu reproduir cap "contingut protegit" en Windows Vista, a causa de la incompatibilitat d'interfícies (S/PDIF).

¹¹<http://www.cs.auckland.ac.nz/~pgut001/>

¹²http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html

¹³http://max-sievers.name/vista_cost.pdf

- Serà habitual patir una pèrdua significativa de la qualitat de l'àudio per culpa de la necessitat de comprovar cada bit del flux multimèdia per saber si és “contingut protegit”.
- La idea de controladors de codi obert serà abandonada perquè el DRM en el seu conjunt es basa en el fet que tot el desxifrat té lloc dins d'una “caixa negra” i només un petit nombre d'empreses escollides poden conèixer-ne l'interior. Això s'anomena **seguretat per ocultació**¹⁴, i el concepte de codi obert és diametralment oposat a aquest.
- Un dels objectius de Microsoft és el d'eliminar qualsevol estàndard de maquinari. Segons la teoria de Microsoft, cal que cada dispositiu es comuniqui amb el sistema operatiu d'una manera única per tal que el DRM funcioni com es vol. Això obligarà a la incompatibilitat entre dispositius, liquidant els estàndards d'interfície existents.
- Els atacs de denegació de servei (DoS) seran una pràctica habitual. La nova era dels atacs DoS serà més danyosa que mai. Això està relacionat amb els *tilt bits* introduïts en el Windows Vista. Un programa maliciós serà capaç d'usar les restriccions del DRM d'una forma apropiada i la detecció de la seva activitat serà pràcticament impossible, o àdhuc il·legal (com ho llegiu!) gràcies a la infame acta **DMCA**¹⁵, la qual prohibeix la utilització de qualsevol tècnica d'enginyeria inversa per tal d'entendre o trencar el DRM.
- L'estabilitat dels dispositius disminuirà a causa del fet que els dispositius no hauran de fer només la seva feina, sinó també de “protegir” (qui? l'usuari no, òbviament) contra l'ús il·legal de fluxos d'àudio i vídeo. Aquesta “protecció” requereix un munt de potència addicional de procés i per descomptat també molts dies de programador. Qui pagarà tot això? Per descomptat nosaltres, els clients.
- La publicació d'aquesta especificació per part de Microsoft sembla ser el primer cas a la història d'un productor de programari que dicta als fabricants de maquinari com han de dissenyar i com han de funcionar els seus productes. Sembla perillós, especialment quan tots prenem consciència de les intencions de Microsoft.

Les conclusions són força entristidores. Si la majoria de fabricants de maquinari com ara Intel, NVidia i ATI es prenen seriosament aquestes recomanacions i les implementen als seus productes, pot passar que el client no només adquireixi un producte d'inferior qualitat (defectuós per disseny), sinó que a més haurà de pagar el cost addicional d'implementar les restriccions DRM (els fabricants probablement no voldran assumir els costos extra per quelcom que no els dona cap benefici).

*Actualització: ja hi ha hagut una resposta de Microsoft a l'article de Gutmann: **La protecció del continguts al windows Vista - Vint preguntes i respostes**¹⁶. Tanmateix,*

¹⁴http://en.wikipedia.org/wiki/Security_through_obscurity

¹⁵<http://en.wikipedia.org/wiki/DMCA>

¹⁶<http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/20/windows-vista-content-protection-twenty-questions-and-answers.aspx>

la defensa és molt pobre. El responsable del programa de gestió del Vídeo al windows Vista (Dave Marsh) va confirmar la major part de les conclusions de Gutmann, però les presentà com a "inevitables" i com a "aportadores de funcionalitat addicional". Els lectors de *OSNews*¹⁷ semblen estar d'acord en què la resposta de Marsh era bàsicament l'acceptació de la culpabilitat.

Fins aquí hem tractat només els costos tècnics del DRM i la computació confiable en la forma proposada pel gegant de Redmond. Però els costos ètics de la "innovació" són encara més interessants... o depriments. Seguiu llegint.

4 DRM i la llibertat, o què diu Richard Stallman i la FSF

Segons *Stallman*¹⁸,

"La DRM és un exemple de característica maliciosa - una característica dissenyada per danyar l'usuari del programari i, en conseqüència, és una cosa amb la qual no hi pot haver tolerància."

Stallman no és l'única persona respectada en el món de les Tecnologies de la informació que creu que la DRM és la maldat pura. Un altre conegut lluitador contra la DRM és John Walker, l'autor del famós article "La censura digital: Com el Gran Germà i les grans *Majors* poden tornar a posar el geni d'Internet dins la làmpada". Walker compara la *Imprimatur* digital¹⁹ amb la DRM a internet i la computació en general.

En el Windows Vista s'ha decidit implementar la **versió més restrictiva de la DRM** mai coneguda. Si els somnis de Redmond es fan realitat i els grans fabricants de maquinari decideixen també implementar la DRM dins els seus xipsets, es pot arribar a la situació en què nosaltres -els usuaris- no puguem decidir sobre el programari per reproduir contingut multimèdia adquirit legalment. I això pot ser només el principi d'allò que podem esperar si no comença una protesta massiva dels consumidors en contra la DRM. En un futur proper pot passar que no puguem executar cap programa que violi alguna de les absurdes patents de programari vigents als EUA o qualsevol tipus de l'anomenada propietat intel·lectual (com si les idees poguéssin tenir un propietari!). I gairebé tot estarà patentat o serà propietat d'algú quan arribi aquell moment.

Tinc una visió de ciència-ficció de la contracultura de les TIC, on el maquinari no contaminat per la DRM només es fabrica a la Xina i la seva utilització és il·legal en molts dels països "civilitzats". I l'únic programari que permet als usuaris fer allò que volen és el (també il·legal) programari GNU, desenvolupat en soterranis pels anomenats "terroristes de les TIC" - hackers del nucli de Linux, antics empleats de Novell i RedHat, esponsoritzats pel Bin Laden de les TIC: Mark Shuttleworth. Sona ridícul? Bé, esperem que sí. Però no crec que Microsoft i Apple protestin quan aquesta visió ridícula i insana es faci realitat...

¹⁷http://osnews.com/comment.php?news_id=17012

¹⁸http://en.wikipedia.org/wiki/Richard_Stallman

¹⁹http://en.wikipedia.org/wiki/Digital_imprimatur

5 Què és tot això i com podeu protegir-vos

Així doncs, quin és l'origen de tot plegat? Sembla que, per a Microsoft, controlar el mercat del programari de la informàtica d'escriptori ja no és suficient. Ara tracten de controlar també el mercat del maquinari. De moment només "recomanant" les seves solucions a les empreses de maquinari externes. Però en el futur, si l'actual lobby pro-DRM té èxit, pot passar que Microsoft i altres grans companyies de programari dictin com s'ha de dissenyar el maquinari. I tot això -evidentment segons la seva argumentació- només per assegurar l'usuari final i protegir la propietat intel·lectual d'artistes i programadors. Aquesta situació és força paranoica. L'hipotètic pacte entre els fabricants de programari, de maquinari i els proveïdors de continguts (RIAA, MPAA) pot alentir la innovació de la totalitat de la indústria de les TIC durant molts anys. També seria la primera vegada a la història que s'introdueix certa innovació tecnològica basant-se no en la demanda dels consumidors, sinó en les necessitats d'empreses grans i influents. Els consumidors (aquells que estan atents als seus drets) no poden estar satisfets de cap manera amb aquest tipus d'acord.

I com podeu protegir-vos d'aquest "pacte diabòlic"?

- ➔ Primer de tot: ignoreu el maquinari i programari que utilitzi tècniques de DRM per restringir els drets de l'usuari. No compreu música, pel·lícules i altre tipus de contingut protegit per mecanismes DRM. Al seu lloc, utilitzeu els serveis alternatius recomanats per la campanya "**Defectuós per disseny**"²⁰. Aquestes són eines i serveis lliures de DRM.
- ➔ En segon lloc: parleu, parleu i parleu una vegada més encara. Feu saber a la vostra família, amics, companys de feina, etc. els perills associats amb l'ús del DRM als productes. Aquesta és la millor manera d'educar la gent en què és el DRM i perquè han d'anar-hi amb compte. A ningú no li agrada que el limitin. Quan la gent s'adoni de les restriccions, no compraran productes que els limitin. Així de senzill.

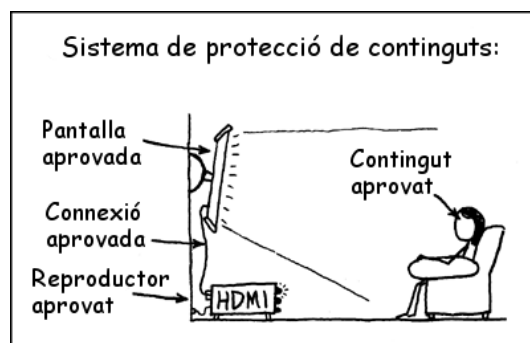


Figura 2: Autor: Randall Munroe. Sota llicència CC-by-nc

²⁰<http://www.defectivebydesign.org/pl/guide>

6 Trencar la DRM – és... senzill

D'acord, i què podem fer si ja hem adquirit legalment alguns continguts (com ara multimèdia o documents de text) protegits amb alguna mena de DRM? No us preocupeu. La majoria de proteccions ja han estat **trencades fa molt de temps**. Per exemple, per poder reproduir DVD xifrats amb CSS en un sistema GNU/Linux podeu emprar gairebé qualsevol reproductor com ara MPlayer, VLC o Xine amb la libdvcss2 habilitada (aquesta és una llibreria no llicenciada usada per desxifrar DVD xifrats amb CSS). Si posseïu música en format AAC (per exemple comprada a iTunes), podeu convertir-la fàcilment a un format més amigable utilitzant [JHymn](#)²¹ i sense perdre qualitat. La història es repeteix per totes i cadascuna de les noves tecnologies DRM que es van introduint, com ara PDF xifrats, Windows Media o, més recentment, el HD-DVD (vegeu [el correu de muslix64 sobre el BackupDVD](#)²²) i el BluRay.

Trencar les restriccions de la DRM és difícil però sempre possible, en virtut del fet que tots els mecanismes DRM necessiten emprar xifrat simètric per poder funcionar. Aquesta mena de xifrat requereix que les claus estiguin amagades ja sia en el maquinari o bé en el programari – en ambdós casos un *hacker* pot accedir-hi, analitzar-les i trobar la manera de desxifrar els fluxos de dades. Si esteu interessats en els detalls de com fer-ho, llegiu l'[informe de Cory Doctorow](#)²³ per a Microsoft Research sobre el disbarat de la DRM.

7 Si però, és legal?

Sabem que podem trencar pràcticament qualsevol restricció DRM emprant programari lliure fàcilment disponible. Però què podem dir de la part legal? És legal fer-ho a casa? Bé, depèn... Depèn d'on esteu vivint. Per exemple, si teniu la mala fortuna de trobar-vos als Estats Units o França, teniu prohibit reproduir la vostra música o pel·lícules adquirides legalment (tal com ho llegiu!) que estiguin protegides per DRM si no compreu també un sistema operatiu aprovat (com ara MS Windows o MacOS) amb un reproductor aprovat (com ara PowerDVD o iTunes). Als Estats Units això està regulat per la [DMCA](#)²⁴. A França, per una llei similar anomenada [DADVSI](#)²⁵.

Afortunadament, en molts altres països, encara és completament legal utilitzar programari lliure per trencar les restriccions imposades pel DRM, com ara usar DeCSS per veure els vostres DVD. Allò que nosaltres, com a persones que donem suport al programari lliure, cal que fem és vigilar constantment els legisladors dels nostres països per tal que no provin d'introduir restriccions similars a les de França o els EUA. A Polònia, per exemple, una protesta liderada per un dels grans portals pro-Linux i milers d'usuaris d'ordinadors va fer que el partit majoritari abandonés el projecte d'introduir una llei semblant a la DMCA a Polònia. Els activistes del programari lliure d'altres països, com ara el Regne Unit, van encara més enllà i proven d'introduir la

²¹<http://hymn-project.org/>

²²<http://forum.doom9.org/showthread.php?t=119871>

²³<http://www.craphound.com/msftdrm.txt>

²⁴<http://en.wikipedia.org/wiki/DMCA>

²⁵<http://en.wikipedia.org/wiki/DADVSI>

prohibició total de la DRM²⁶ en el sistema legal Britànic.

Òbviament, trancar les restriccions és lluitar contra els efectes, no les causes. El problema real és el fet que la DRM existeix i que és àmpliament acceptada per la (ignorant) majoria. Si els usuaris d'ordinadors no s'uneixen i protesten contra la inclusió de la DRM en més i més productes, ningú no ho farà, i la DRM esdevindrà el nostre pa de cada dia contra el qual haurem de lluitar com ho fem ara amb els virus i programes maliciosos. Aquest any pot ser l'any en què es prenguin les decisions importants, tant per part de la indústria (si incorporar o no la DRM als seus productes) com per part dels usuaris (si acceptar o no la DRM tal qual). Si perdem aquesta batalla, haurem d'acceptar allò que ens vingui. Crec que no ens podem permetre perdre. Ho creieu vosaltres?

8 Més informació sobre la DRM

- [Defective by design](#)²⁷ – La campanya anti-DRM
- [BadVista.org](#)²⁸ – Campanya de la Fundació pel Programari Lliure contra Windows Vista
- [The Right To Read](#)²⁹ – L'article de Richard Stallman
- [Can you trust your computer?](#)³⁰ – Un altre article de Stallman sobre la "computació confiable"
- [Digital imprimatur: How big brother and big media can put the Internet genie back in the bottle](#)³¹ – Un famós article de John Walker
- [RealNetworks reply to Linux: DRM or die!](#)³² – La reacció de RealNetworks a l'anunci que Linux no suportarà DRM
- [Linus on DRM](#)³³ – Linus Torvalds no protesta contra la implementació d'algunes tècniques DRM al nucli de Linux (sempre i quan es puguin desactivar)
- [A Five Minute Guide to Opposing DRM](#)³⁴ – L'article de Bruce Byfield sobre una manera intel·ligent d'oposar-se a la DRM
- [The big DRM mistake](#)³⁵ – Scott Granneman parla sobre l'error global del concepte DRM

²⁶<http://petitions.pm.gov.uk/bandrm/>

²⁷<http://www.defectivebydesign.org>

²⁸<http://badvista.org>

²⁹<http://www.gnu.org/philosophy/right-to-read.html>

³⁰<http://www.gnu.org/philosophy/can-you-trust.html>

³¹<http://www.fourmilab.ch/documents/digital-imprimatur/>

³²<http://arstechnica.com/news.ars/post/20060410-6569.html>

³³<http://yro.slashdot.org/yro/03/04/24/1312231.shtml?tid=106>

³⁴<http://interactive.linuxjournal.com/node/1000073>

³⁵<http://www.securityfocus.com/columnists/390>