Digital Rights Management

Past and Present

Ben Wells

Digital Rights Management: Goals

- To extend "analog" copyright techniques to the digital world.
- Give content Creators some control over the use of the media they produce.

Applications where DRM is present:

Basically every single major digital media distributor!!

Different Generations of DRM:

Generation 1 (80's, early 90's)

- Sensitive Material wrapped in container file. (ex. zip, pgp (pretty good privacy) files)
- Container is encrypted with a key or password.
- PGP often uses RSA & hash functions
  - public-key encryption system.
  - Digital Signature provides authentication
  - hash function guarantees that the contents have not been tampered with.

Different Generations of DRM:

Generation 2

- Native Files encrypted within a native application (based on shared password)
- Access Control Permissions added
  - disable print, copy
  - number of views
- Permissions the same for all users. File based.
- Problem: shared passwords can be, well....shared.

Different Generations of DRM:

Generation 3

- AC Permissions can now vary with each user
- Each transaction generates a private key known only by the user who purchases the content.
- Problem: Permissions are difficult to change once the file has been sent to user.

Different Generations of DRM:

Today:

- AC, Authentication, Permissions moved from native application "into the cloud"
- Server maintains list of policies that map users and groups to permissions.
- Permissions can be dynamically managed.
- User's Actions can be logged and recorded.

DRM History: A Brief Timeline

- 1983 - 1998
  - Software: Most digital content was stored in password-protected container files.
  - Hardware: CD's and DVD's used DRM techniques to prevent copies from being made.

1998
Digital Millenium Copyright Act (DMCA)

- First legislation aimed to curb illegal piracy of digital media.
- Made illegal to circumvent DRM or otherwise bypass any access controlled media
- Made DRM Circumvention tools illegal

Copyright gone wrong
Sony Rootkit Scandal of 2005

- Sony once included a rootkit in every CD they sold.
- Allows user information to be sent to Sony.
- Problem: Hackers could manipulate this code to work for them maliciously.
- Initial public response: "Most people, I think, don't even know what a Rootkit is, so why should they care about it" *Thomas Hesse, Sony CEO*

Just an example of how DMCA protects consumers as well as content providers

First Response:

- 2001: Rhapsody reveals subscription-based, unlimited music streaming service.
- Allows customers to manage personal "libraries" without actually downloading files.
- RealNetworks follows example in 2003

2003 iTunes

- First Digital Music Store
- All files protected with FairPlay DRM

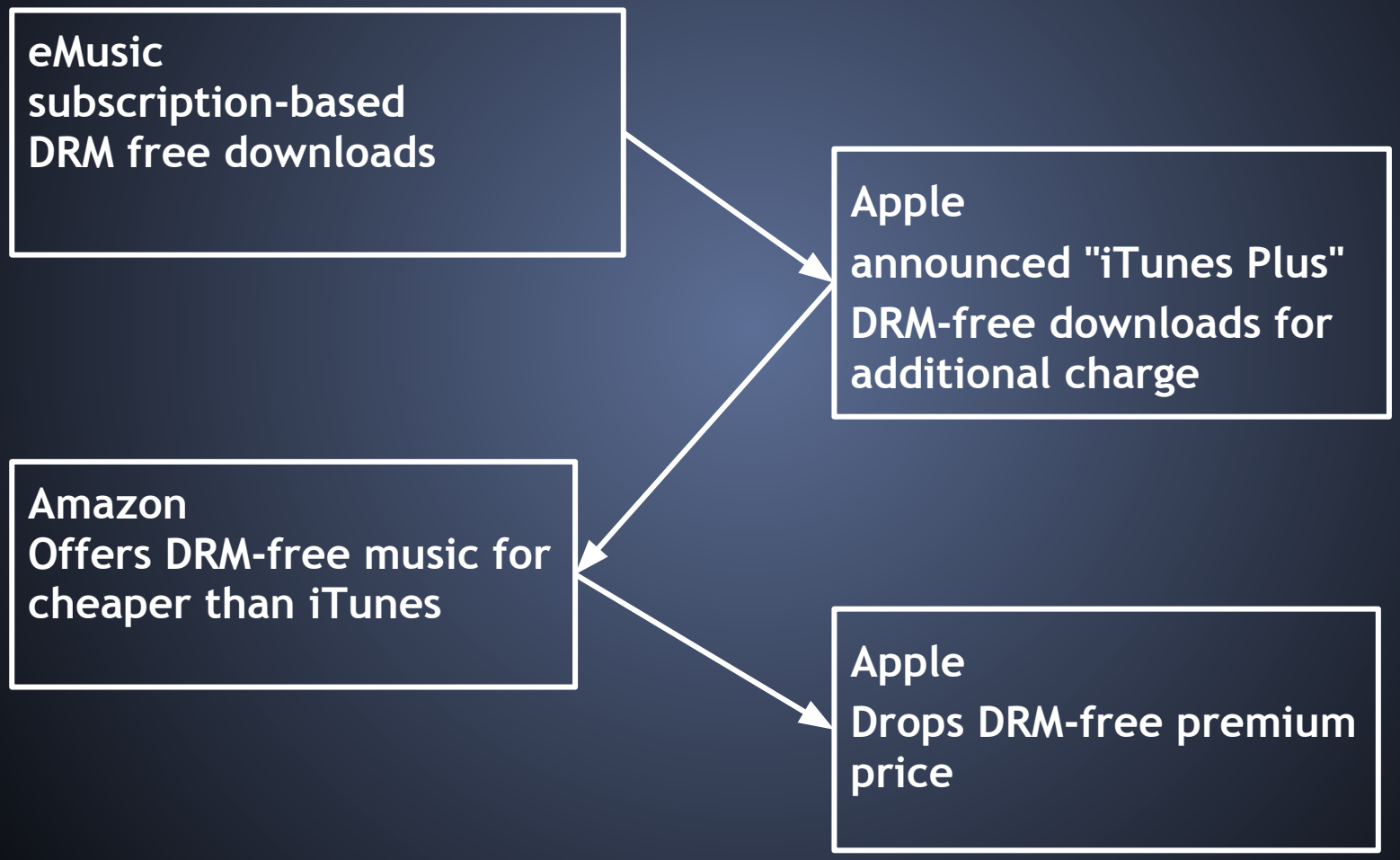
Restrictions

- Downloads can only be accessed from 3 authorized computers.
- Users cannot make more than 10 copies of a CD.

Example Followed

- By 2006, Apple controlled 88% of the legal US music download market
- Next step for competitors: Offer DRM-free downloads.

Market-Share call and response



2009

- All music sold on Amazon and Apple's iTunes will be offered DRM-free
- Apple: Users can convert previously purchased music for a small fee ($.30/song)
- Marks "Death" of DRM-protected Audio
  - Video, Apps, Audiobooks, and eBooks still remain protected.

How FairPlay DRM works:
List of authorized machines for each user kept on servers.

User Creates iTunes Account

User: jsmith1234
Password: *******

Generates Unique authorization ID:

74FB-89GT-5T67

List of Authorized Machines (up to 5)

1. ....
2. .....
3. .....

Apple

User: jsmith1234
Password: *******

User: jsmith1234
Password: *******

How FairPlay DRM works

User

Apple

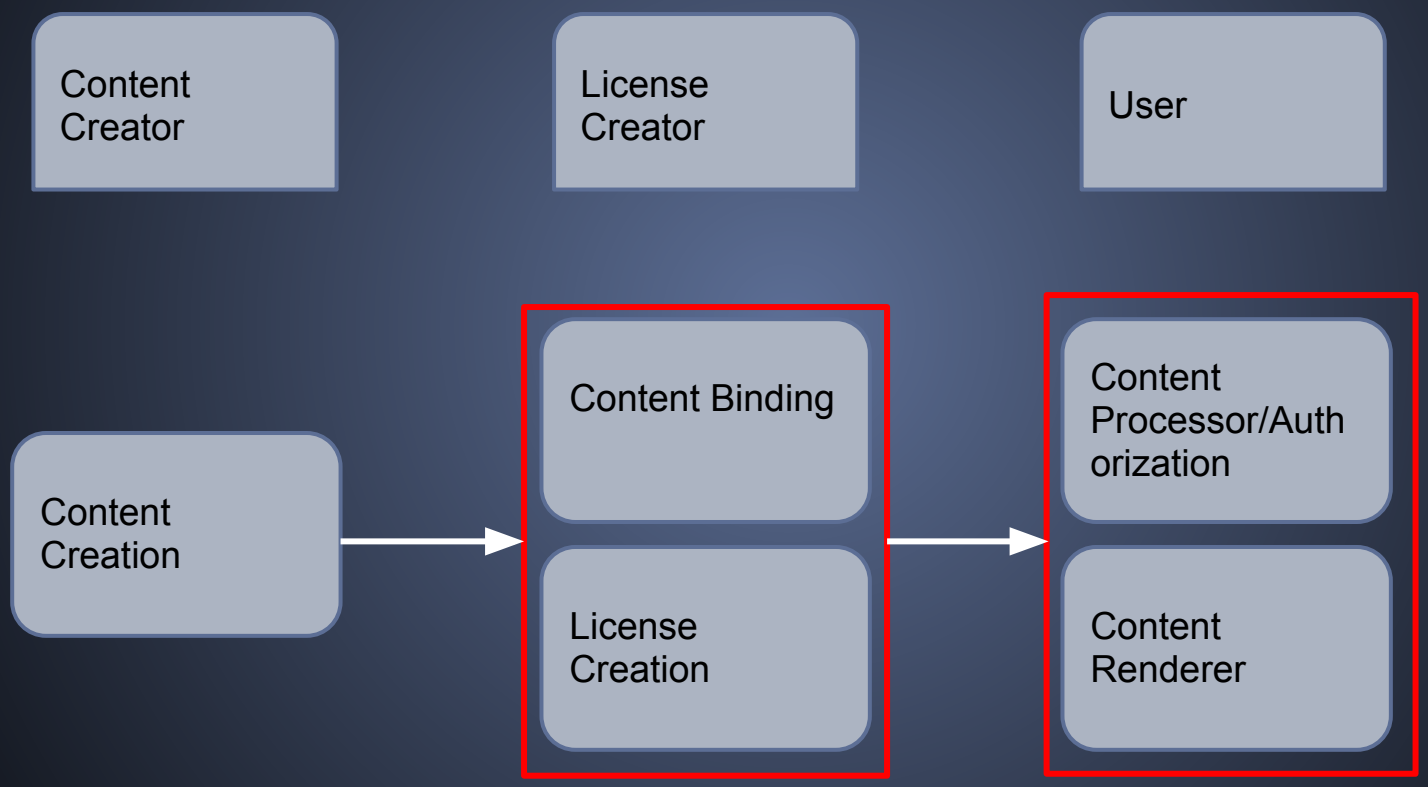
1. Media Purchased from iTunes Store.
2. Unique, File-Specific User Key Generated Locally
3. One copy of user key stays on local machine
4. 2nd copy sent to Apple Servers along with proof of transaction

5. Transaction and User key logged
6. File encrypted with Master Key sent to user

7. File Authorized and decrypted with User Key

Note: All key generation and decryption is done locally. This minimizes relying on the network to authorize users for each purchase and speeds up transaction time significantly. A list of keys for each file is stored locally, on Apple's servers, as well as on any iPod or iPhone containing the media files.

DRM Basic Concepts



DRM Basic Concepts Cont...

Access Control

- Operates on a Mandatory, Implicit Deny Policy
  - Access is denied by default unless user is explicitly authorized.
  - permissions granted to user can vary from user to user
    - Allows for Premium Services
    - Varied price points

DRM Basic Concepts Cont...

Enforcing the Three Security Requirements:

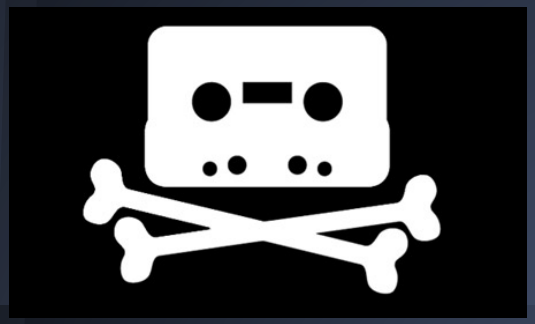
1. Integrity: It needs to be guaranteed that content is accessed by untampered software/hardware developed by official content creators.

2. Availability: Creators need to precisely deliver what has been requested, in a consumable form, at the desired time for the user.

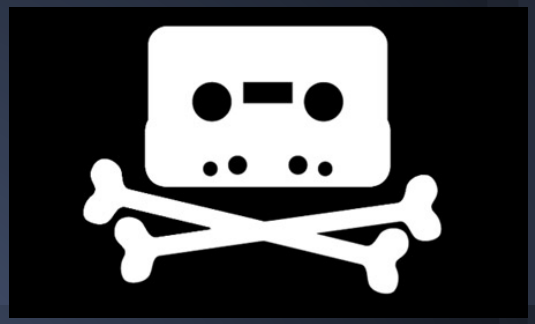
3.Confidentiality: The license creator must only save the personal data for which the user has given permission and only use this data for purposes for which the user has given permission.

Project Contributions:

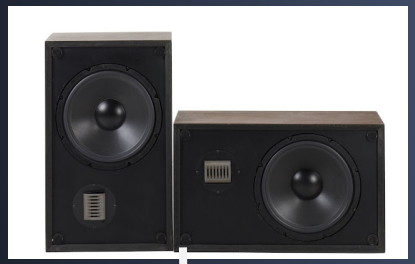
- Analyze DRM circumvention methods of audio.
  - How they were done in past vs. present
  - Use results to form conclusions about other forms of media
- Gather facts about the music industry and DRM, including consumer attitudes from previous research.
- Perform a risk assessment and threat analysis to:
  - Forecast what will happen with DRM and other forms of media.
  - Suggest possible solutions based on potential forecast paths.

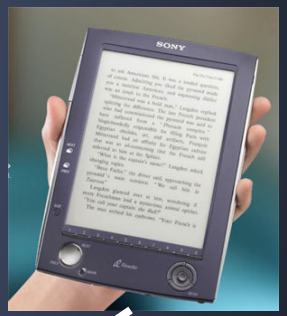


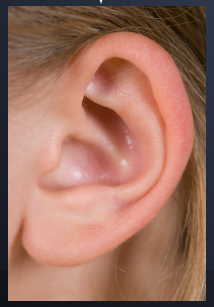
Analog Hole

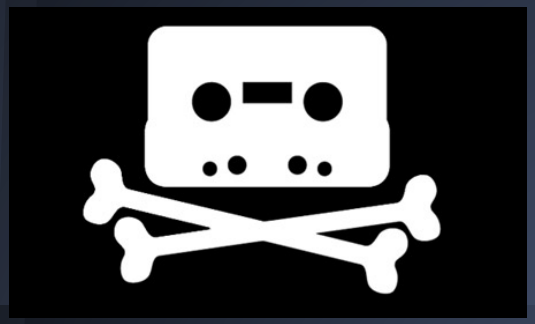


In order for digital media to be consumed, it must first be converted into an analog signal.

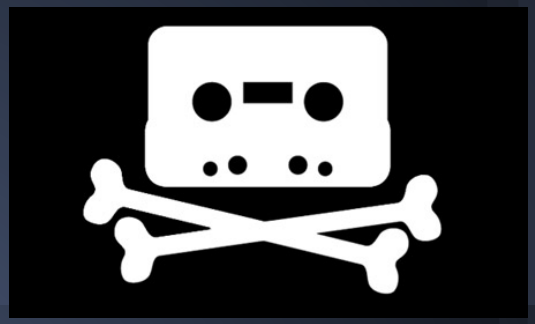






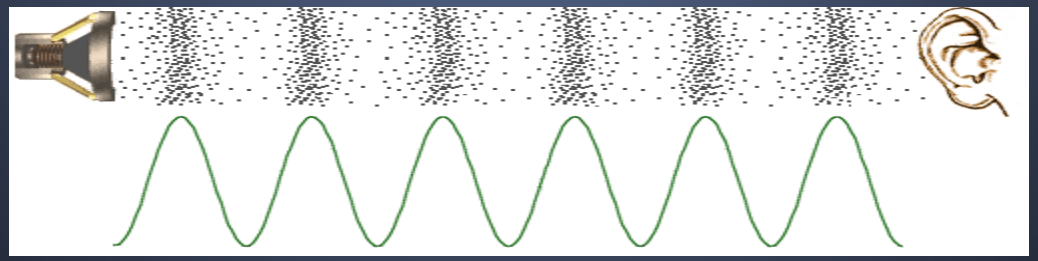


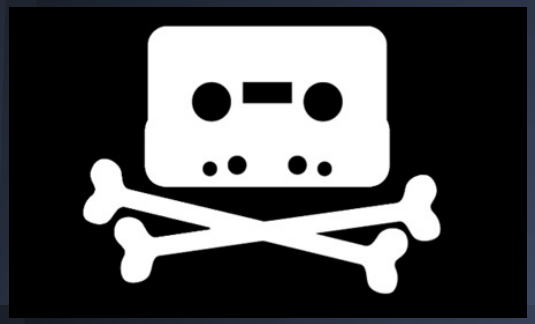
Analog Hole



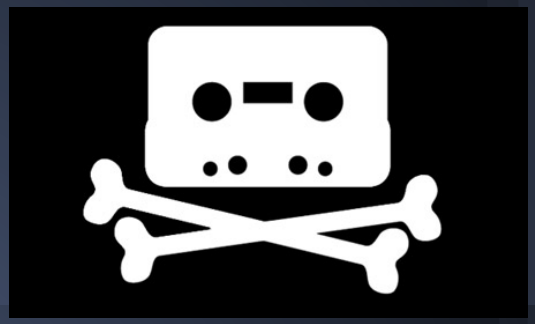
<u>Problem:</u>

This signal can be intercepted, recorded, or otherwise replicated. Creating a copy of the original.





Analog Hole



The analog hole is unavoidable.

A simple byproduct of human beings consuming digital products.

DRM can't "fix piracy" because there will always be ways around it.

What Else Went Wrong?

Vs.

Adaptation vs. Resistance

- In the case of the music industry. Consumers began to demand digital music.
- The music industry was not prepared
- Record companies and media producers chose resistance over adaptation.

What Consumers wanted:

Digital audio, anywhere.

What was sold:

DRM-Restricted audio

Radical Thinking

Open Music Model (2002)

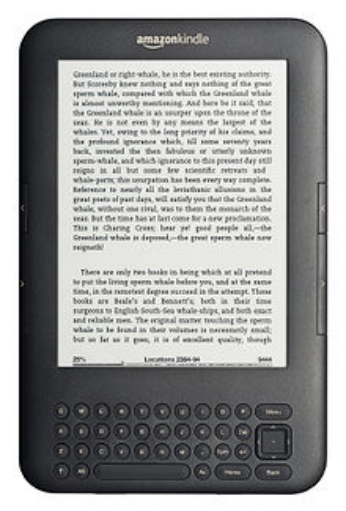
The only way for DRM to be successful is if there existed only one, universal system used by all content creators.

Problem: Market is already too segmented.

Apple, Amazon, Microsoft, etc...

Amazon Kindle

Solution that combines DRM Protection with Consumer demand.



Why does it work?

Cross-Platform Support

photo source: amazon.com

Example 2: Netflix

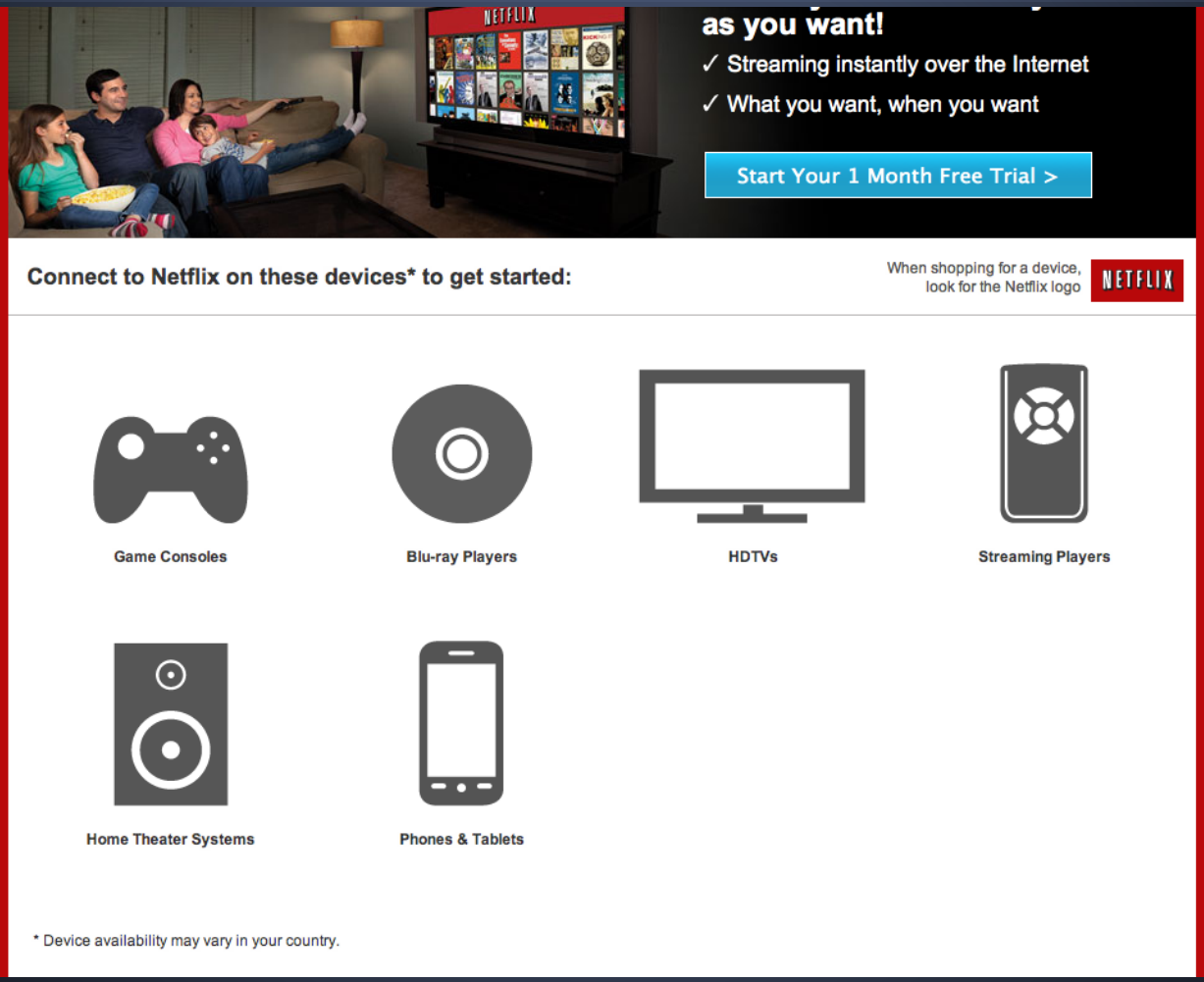


photo source: netflix.com

Is there still hope for music and DRM?

Best Attempt: Amazon Cloud Player

Enjoy your music anywhere

Play or download your music from the cloud with Amazon Cloud Player, available on the web, Kindle Fire, iPad, or Android device. Browse and search your library, create and manage playlists, stream your music from the cloud, or download it for offline playback. Launch Cloud Player for web, or learn more about how to use it on your favorite device.

Upload your music collection

Get the benefits of Cloud Drive for your whole music collection by uploading it from your computer. Right now, you can get unlimited space for your music in Cloud Drive, plus 20 GB of storage for your other files, for just $20 each year. Saving your Amazon MP3 purchases doesn't count against your quota. Learn how to upload, or upgrade to an unlimited plan.

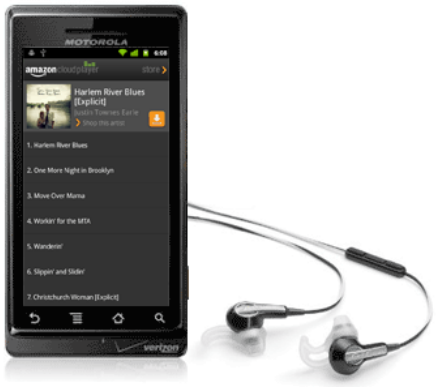


photo source: amazon.com

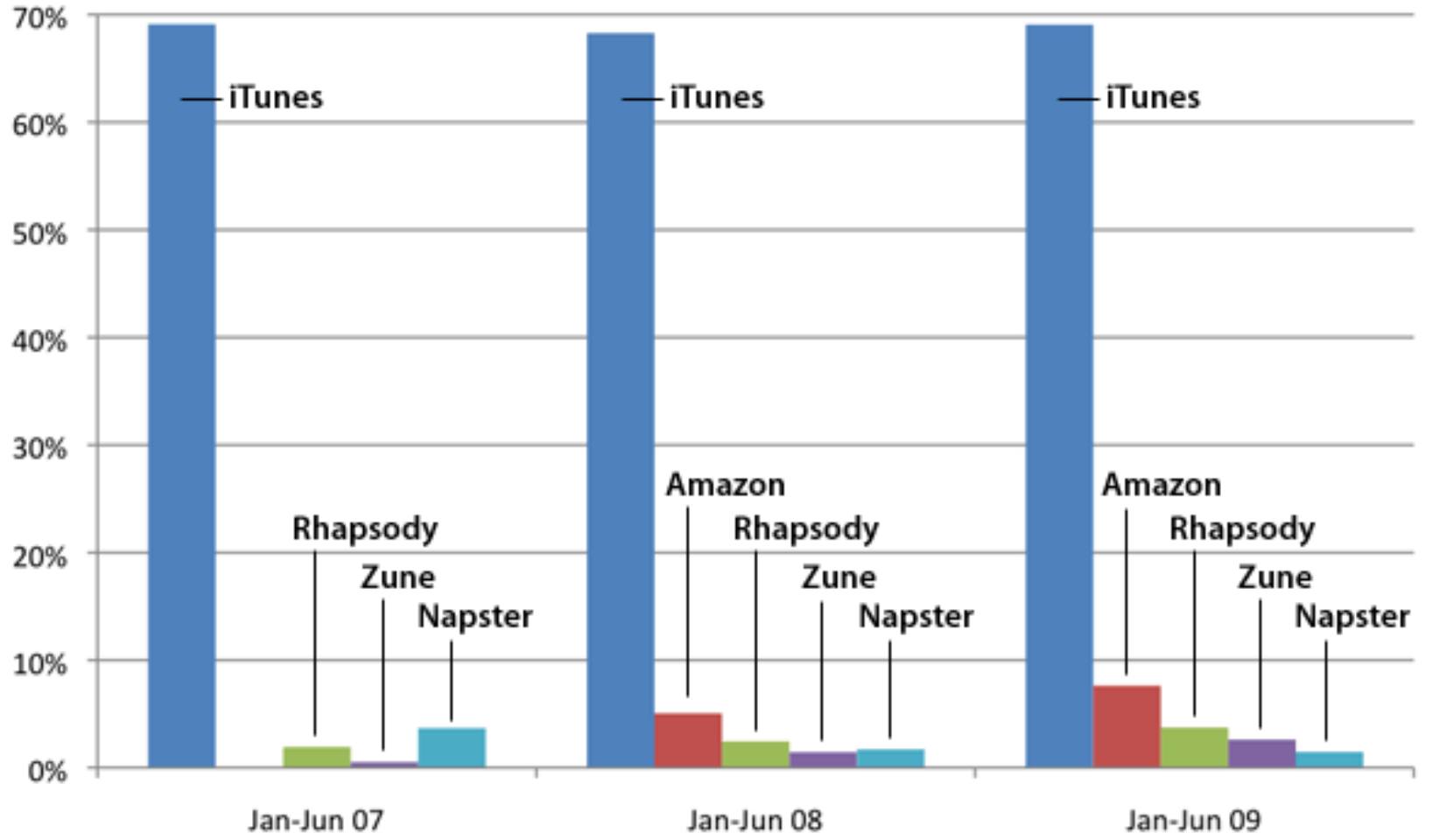
Problems:

1. There has been so much uproar about DRM-protected music that it has already been removed from audio sold on Amazon. (Too late to bring it back)

2. Apple and iTunes

Silicon Alley Insider Chart of the Day

Digital Music Sales Market Share



Source: NPD Group

iCloud

This is the cloud the way it should be: automatic and effortless. iCloud is seamlessly integrated into your apps, so you can access your content on all your devices. And it's free with iOS 5.

Learn more ›

Watch the new TV ad ›

iTunes in the Cloud. Your music on all your devices.

All of your devices?

photo source: apple.com

Reality:

iCloud lets you play music on all of your devices

if and only if

all of your devices are Apple devices.

also:

Amazon Cloud Player not allowed in Apple's App Store

Final Thoughts

Too Late for Music Industry?

Final Thoughts

The bright side: Knowledge gained.

An example has been set for other forms of media.

References

Haber, S., Horne, B., Pato, J., Sander, T., & Tarjan, R.E., "If Piracy is the Problem, is DRM the answer?", In *Digital Rights Management: Technological, Economic, Legal and Political Aspects,* ed. Erberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump, Springer-Verlag, 2003.

Jonker, H.L., Mauw, S., Vershuren, J.H.S., & Schoonen, A.T.S.C. (2004, June). Security Aspects of DRM Systems. 25th Symposium on Information Theory in the Benelux: The Netherlands.

Loebbecke, Claudia, Bartscher, Philipp, Weiss, Thomas, & Weniger, Sandra. (2010). Consumers' Attitudes to Digital Rights Management (DRM) in the German Trade eBook Market. IEEE Ninth International Conference on Mobile Business.

Mauw, S., & Jonker, H.L. (2007). Core Security Requirements of DRM Systems. ICFAI Book series, ICFAI, India.

Sicker, Douglas C., Ohm, Paul, & Gunaji, Shannon. (2007). The Analog Hole And The Price of Music: An Empirical Study. Journal on Telecommunications & High Technology Law.

Smith, Matt, Wilson, Lakaii, & Gunaji, Shannon. (2005, August). Sidestepping DRM: A Look into the Analog Hole. University of Colorado at Boulder. Retreived from http://en.scientificcommons.org/43486934.

Stamp, Mark, Sebes, E. John. (2007). Solvable Problems in Enterprise Digital Rights Management Information Management & Computer Security.

References

Suehle, Ruth. (2011). The DRM Graveyard: A Brief History of Digital Rights Management in Music. Red Hat, Inc. Retreived April 1, 2012 from http://www.opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music

Torres, Víctor, Serrão, Carlos, Dias, Miguel Sales & Delgado, Jaime. (2008, June). Open DRM and the Future of Media. IEEE Multimedia, vol. 15, no. 2, pp. 28-36.

Watermarking World (2009), "Digital Watermarking", http://www.watermarkingworld.com/digital_watermarking. Accessed 5 April, 2012.

Thank You!