TCB and DRM

A technical, economic and social look at the feasibility of DRM

Written by Martin Häcker as part of the seminar “Trusted Computing Base” jointly done by KBS and IG at the TU-Berlin.

Executive Summary

"We have Ph.D.'s here, that know the stuff cold, and we don't believe it's possible to protect digital content." -- Steve Jobs, Rolling Stone Interview (2002)

In this paper I am going to show that techniques to ensure the correct abiding of copyright restrictions are inherently flawed and will not work. To do this I have to bring together technical, social and economic reasons. This is unfortunate, as it makes the problem much harder to describe and understand, but it is also unavoidable as the problem itself is inherently anchored in all those fields.

Outline

Free vs. permission Culture

To prevent being lumped together with people who just want to get everything for free, I'd like to establish a few distinctions.

First, what we currently have, or at least had at some point in our society was a free culture. As Lawrence Lessig describes in the preface of his book "Free Culture" (Lessig, 2004), a free culture is about free markets, free speech, free enterprise, free elections and many more "free's". This of course does not and even should not mean that there is no value and price in this system, or to quote Lessig again: "just as in a free market not everything is free" (Lessig 2004, p.xiv). In the ideal of a free culture this facilitates what Isaac Newton meant when he said "Standing on the shoulders of giants." by being able to build on the work other people have done before.

Second, a permission culture is in some ways the opposite. In part we have that already, but most of it is still in a future we hopefully won't get. In such a future, free speech and free markets are not anymore. Instead the owners of old copyrights can control who creates and innovates after them, as the copyrights no longer expire. This, to speak with Newton again, allows them to control who will be able to stand on their shoulders.

The important distinction between those two kinds of culture is their focus, or what they seek to optimize. The permission culture optimizes for wealth and control of those who already are powerful. This in itself is not bad, but the implication of it is, namely that it does not optimize for global scientific, artistic and economic progress. This is exactly what the free culture seeks to optimize, which is the very reason why it seems logical to me for a society to prefer it.

The ways in which a free culture is different from a permission culture are very powerful yet at the same time surprisingly subtle. To prevent the free riders[1] problem, the society grants creators an intellectual property.[2] In other words it is a monopoly on the use of what they created.[3] To prevent a permission culture it limits this monopoly so that it ends after a specific term and only covers specific uses. For these reasons it enables other creators to build on that work.[4]

[1] The free riders problem in essence means that some people benefit from the work of others without contributing something to it. In the context of content creation this means that if it is possible to get content for free, without paying the artist. Artists will be less motivated to create content. This goes on to a point where the artist has no motivation left and therefore the content is not created. (Stanford Encyclopedia of Philosophy)

[2] Europe and especially Germany has a very different intellectual property system than the USA, the most important difference being that you cannot sell it. In this article, if not explicitly stated otherwise, the American copyright system is meant.

[3] Of course this includes the ability to license the work to selected parties. The problem though is the word selected in this, as it means there is no equal access to the content in question.

[4] This interestingly enough is exactly the same line of reasoning that led to the patent system, yet sadly these systems are not unified.

There should be a balance between giving those who create an incentive to do so and ensuring the possibility for others to create. This balance is adjusted by the length of the term that the monopoly of the past creators holds.

To summarize this: I do not propose a culture in which everything is free, which I think is no more desirable than needing a permission to build on anything. What is needed is a point between these two opposing points of view, which is what a free culture is.

Why is DRM wanted?

Let's assume for a moment that there could be a DRM system that worked and that this system were in use by everybody. Corporations clearly love this thought. While in the analog world, after you sold e.g. a book, the customer owned it and you could not do anything about him reading it as often as he wanted to. Also there was no legal ground on policing this very fact. Now in the digital world, all uses of a digital good technically require a copy to be made of it. For example, to read an e-book it needs to be copied from the hard-drive to the RAM and from there it is rendered, and then copied to a viewing device, be it a printer or a monitor. This implies that the copyright law can now be used to enforce arbitrary restrictions on these actions – which is a big enlargement of its scope. What follows from this line of reasoning is that songs you buy can only be played thrice or only on your birthday. CD's you can only play in your home stereo and not on your computer or in your car. And of course you cannot use those songs as a ringtone for your mobile.[5]

Of course, there are radically different ways in which a society could try to compensate its artists for the content they create. For example if you view the ability of the artists as a gift like a property and also take into account that property has its duties, then you end up at the question to which amount artists perhaps should be obliged to give up rights to their creations to benefit the society at large.

This of course brings with it the very hard problems of defining the precise meaning of when something is published and what rights the society should have on created, published or sold works.

These problems need to be addressed though to start speaking about a "content flatrate" as I will later do.

Clearly this control enables a lot of new revenue streams. In essence DRM technology on the one hand and copyright law on the other enables a content publisher to determine exactly under which conditions his content can be rendered. Music that only plays on mobile phones from Sony-Ericsson, but not others is just as possible as music that can only be played on one of your devices, but nobody else's. For example Apple uses DRM technology to assure they are the only (monopolistic) seller of music for its popular iPod platform.

Economists speak of lock-in in these contexts, which means the customer cannot easily switch to another provider or that he has to consider the opportunity costs of the change. Of course from the point of view of a corporation this is very desirable, as you can bind the customers to you and your platform and prevent them from straying to the competition. This in turn enables corporations to

[5] As was argued by Mako Analysis (2004) in a report that said in essence that the customers' ability to use arbitrary mp3's as ringtone on their mobile is harming the ringtone industry.

have business models that make them more money without having to fear competition as much. For the customer it means he has to calculate the opportunity-cost of changing his business partner into the eventual gains the change would give him.

This is what makes old business models like club or subscriptions viable. For example Jamba sells subscriptions to ringtones. It would probably be considerably harder for them to do business if it was very easy to get arbitrary sound files to be used as a ringtone on a mobile. Pay per view or renting of content is much harder to sell to customers if you could become the same content somewhere else for a flat fee or for free.

Of course a working DRM scheme also means that the Industry does not have to fear that “the blood is sucked out of their veins” (Daniel Somers of AT&T) by the darknet (Biddle et al., 2002) or more mundanely: public file sharing networks. Currently this is touted as one of the big reasons why DRM technology is needed and should perhaps even be mandated by law.

To summarize this: Publishers would like DRM technology to prevent piracy of their products and create more customer lock-in, as that would allow them to charge them more money.

The technical foundation of this dream

There are three basic problems with piracy that a technological solution has to factor in: unauthorized acquisition, unauthorized use and their enforcement.

Unauthorized acquisition means downloading a file from a peer-to-peer network, or otherwise getting a piece of content in illegitimate ways. Unauthorized use means the consumption of said piece of content without having paid for it. Enforcing those rules means that the system on which the rules evaluating engine runs needs to be as secure or trustworthy to the content providers as possible.

There are basically three approaches to the problem of unauthorized use and acquisition (or just short DRM) – Watermarking, fuzzy hashing and secure containers (Haber et al 2003). Out of these watermarking and fuzzy hashing could address both unauthorized acquisition and use, while secure containers only address the problem of unauthorized use. All of them in turn rely on the presence of a trusted system to protect them.

A short discrimination of Trusted and DRM Systems

Trusted Computing and Digital Rights Management (DRM) systems are not the same thing, contrary to what many people think.

The central idea behind a trusted system is for it to have a piece of hardware that can monitor all accesses to a specified part of the system and allow or disallow them on the basis of whatever policy is wished for (Anderson, 1972). The trusted systems of today use this concept by supplanting it with chips like the TPM from the TCG to provide a "core root of trust" and a minimal set of operations and storage (Kuhlmannn, Gehring, 2003) to enable this reference monitor to be implemented on an otherwise normal personal computer.

To summarize this: a reference monitor is tamper resistant, cannot be bypassed and is small enough for complete validation. It is also the heart of a Secure Computing Base that can now be built up around it.

The central idea behind a DRM system though is quite a bit more complex. It also has sort of a reference monitor at its heart that monitors the access to digital content, and it also has the power to prevent this access if it 'thinks' that the user has not enough privileges to use it. However to work effectively a DRM system also needs two more databases than a TC system. It needs one that stores all the digital rights that apply to content and then another one to store the accounting and billing data generated by the use of the content.[6] With these additional databases the DRM system is able to monitor access restrictions, copy restrictions or the use of content. It is also able to store and report accounting and billing information.

To summarize this: a DRM system is very policy specific. It has all the defining qualities of a reference monitor, but adds to it many operations to enforce machine governed rules for use of creative works. (Stefik, 1999, p.55)

The contrast between a mere trusted system and a DRM system becomes obvious now. Trusted systems per se are policy neutral, that is they can implement any policy, while DRM systems are very specific in implementing policies to enforce digital rights. DRM systems use and need a trusted system as a building block to become effective. DRM systems manage content, while trusted systems manage resources. (Kuhlmann, Gehring, 2003)

So trusted systems are not the same thing as DRM systems, however they can be used to implement them.

Watermarking

A watermark is a piece of information embedded in the normal content. Its defining quality is that it is imperceptible by humans, though still detectable by machines. To do this there needs to be bandwidth left in the compressed content that is not needed for the content itself. If that is the case (and it will be for the foreseeable future,

[6] Of course this data will likely be spread around in the system, for example the billing data could be stored with the vendors, or encoded into the fact that a piece of content is sealed to a specific machine, while the digital rights data will in some cases be stored inside the content files directly. However the data that is held in those databases needs to be accessible to the DRM system.

thanks to our incomplete theory of human perception) this bandwidth can be used to insert a moniker that either identifies the license used for this piece of content or the user who bought it.

The human perception model
A model of human perception is used to lossy compress sound and video far beyond what is possible by lossless compression, without significantly degrading the compression quality.

In sound compression, a psycho-acoustic model does this by describing "how a sharp clap of the hands might seem painfully loud in a quiet library, but hardly noticeable after a car backfires on a busy, urban street. It might seem as if this would provide little benefit to the overall compression ratio, but psycho-acoustic analysis routinely leads to compressed music files that are 10 to 12 times smaller than high quality original masters with very little discernible loss in quality." (Wikipedia, Psychoacoustics)

Usual attacks on watermarks are:

- Transcoding the content from one format to another or even re-recording the content, either digitally (perhaps at the level of the device drivers) or in analog form, by putting a recording device in front of the computer when it renders the content. This attack is usually called the “analog hole”.

- Scaling, cutting or somehow else changing the content in such a way that the watermark becomes unreadable, though preferably its perception by humans is unchanged.

- If the watermark differs from file to file, that is if the buyer’s identity is embedded in the watermark, averaging those files also is a viable way to get rid of the watermark.

At least theoretically it is possible to design a watermarking scheme that could survive the first and the second attack. As for the third attack: it means that embedding personalized information via a watermark is just not feasible.

As watermarking relies on a incomplete theory of human perception to work, it is not possible to assert how much security from attacks it can provide. However, empirical evidence suggests that removing watermarks results in a perceptually degraded signal. Commercially or academically provided watermarking schemes till today have proven to either only address some attacks, or were broken when challenged. (Craver 2001)

So watermarking protects against unauthorized use directly by embedding a watermark detector into the player. It can also be used to protect against unauthorized acquisition by embedding the detectors everywhere in soft- and hardware (especially peer-to-peer file sharing applications but also in firewalls and routers). But this very abundance of detectors could easily be used in algorithms that try to remove the watermark.

Fuzzy Hashing

This is a relatively new concept of content protection. The essence behind it is that the content becomes the watermark. This is done by computing a hash of the content file that has the quality of assigning the same hash value to everything that we as humans perceive the same. This of course also relies on the model of human perception, only this time, the better the model is, the more accurate the fuzzy hash will be.

Ideally flipping some bits will not change the hash value, though the primary attacks against fuzzy hashes are the same as against watermarks. If the model of human perception is good enough though, changing the content so much that it no longer has the same hash value should significantly degrade the content's quality.

Two projects are currently in wider use in this area: Fraunhofer's *Audio ID* and Relatable's *TRM*. The latter is used as the basis for the MusicBrainz open music metadata database. Fraunhofer claims that its Audio ID algorithm "... is resistant to various changes of the raw material, e.g. bias, equalization, acoustical transmission or mp3-coding. Similar to the human recognition ability, being surprisingly exact even with a low signal quality, Audio ID turns out to be resistant to strong acoustic distortions. The identification rate averages out at 99 percent." (Fraunhofer 2004). Relatable claims for their algorithm that it "...has demonstrated 99.4% accuracy at identifying millions of individual audio files. Accuracy rates are warranted for MP3 files at 96 kbps and above or the equivalent such as 64 kbps Windows Media Audio files. For streaming media analog broadcast recognition, observed accuracy rates exceed 98%." (Relatable 2003).

To test a working TRM installation, go to musicbrainz.org and download their free and open source client.

How robust this technology will prove to be against attacks can not be said today, as this technology is still too young. But if it is to be used it needs to be very precise, yielding (almost) no false positives or business and private users will not be able to render legitimate (or even public) content.

Also this technique needs constant access to a database, either remote or local, to check if a computed hash value actually belongs to a protected song. This is of course quite a problem for unconnected small devices with limited storage capacity and no solution for this problem is in sight.

So fuzzy hashing does protect against unauthorized use and acquisition in the same way that watermarking does. However, it adds the problem of access to a database that it needs to decide if the content in question has a license attached to it or not.

Secure Containers

This technique is referred to by a multitude of names. The Trusted Platform Group for example calls these "bound" or "sealed" files (TCG 2004). The term "secure containers" ordinarily refers to any DRM scheme that stores the content in an encrypted form and perhaps prepends something that describes the license granted for this file. This of course shifts the problem from managing the license to managing the keys to these files. Since the user eventually needs to get access to the files trusted platforms are often used to protect the keys with tamper resistant hard- and software. If this works, the trusted platform can be used to check for various conditions which govern whether the content will be rendered or not.

This technique is great in targeting specific users and devices. Apple for example uses this technique to restrict the use of music files bought from the iTunes Music Store to only be played on up to five computers or iPods owned by the buyer.

Usual attacks against secure containers are:

- Tricking the license evaluating engine into releasing the content in an unprotected form, for example by changing it.
- Getting access to the keys used to decrypt the content, e.g. if a TPM is used, by physically hacking the Trusted Platform Module where they are stored.
- Attacking through the analog hole. This is almost trivially easy, as at some point the content has to be decoded to some sort of waveforms for us humans to percieve. Also the term "analog hole" is a bit too harsh in this context, as most of the time the data can already be grabbed at the level of the device drivers or even earlier.

The strength of the secure container method is determined completely on the strength of the trusted platform used to implement it. That is, if the platform is secure then the secure container or "sealed document" will also be secure. Yet, this technique is completely open to the analog hole and only to a limited degree protecting against physical hacking. For these reasons, it is the DRM technique that is the "easiest to defeat" by the determined adversary.

It's also interesting to note that secure containers alone cannot deal with the problem of piracy, as this technique only deals with unauthorized use of content and not at all with unauthorized acquisition. Unauthorized acquisition technically should be no problem, since it is impossible to play secured content, but because it is so easy to get rid of the protection via the analog hole it does not solve the problem.

General Attacks

Typically the license evaluation engine is executed on a computer owned by the customer, not the content provider. On this platform the user needs to be identified to somehow determine that he is in fact allowed to render some content legally. While authentication systems are well understood, it is still another vector of attack against all of the DRM schemes to trick the license evaluation engine into thinking that a different user with more privileges is trying to access the content.

Another attack is getting the content even before it is protected. This attack is commonly used today against movie studios to get movies out on the internet in DVD quality, even before they officially appear on DVD.

Also as I noted with secure containers the security of all DRM schemes completely relies on the security of the platform they are implemented on. In turn, trusted platforms, as they are represented by the Trusted Computing Group, base their security on secure hashing functions like SHA1 and MD5. These cryptographic hash functions are completely different from fuzzy hashing in that flipping even one bit in a file (should) result in a completely different hash value for it. But for some months we have had to consider these hash functions as broken - with no alternative at hand. To quote cryptography researcher Prof. Dr. Ernst-Günther Giessmann from the HU Berlin (Giessmann 2005) “It will be possible to compute arbitrary collisions on a home computer in one evening.” While this is questionable, history has shown that the time between successful attacks against cryptographic algorithms has always shortened exponentially, so the probability that he remains right is pretty high.

Even with the currently still prohibitively high cost of computing preimage attacks [7] people already start to dream about distributed computing projects that try to find the padding needed to make an open source boot-loader appear to the Trusted Platform Module as the signed Microsoft Secure Startup boot-loader (or whatever is needed). With this boot-loader it would be possible to start a different operating system (say FreeBSD) and from there decrypt all the media available with the keys of this system. Or even easier, to make a small ‘decrypter’ appear to the OS as the secure player and do all the decrypting in this program. Still this is some time away, even if it may be only till the end of the year 2005.

To summarize this: While attacks against all the individual techniques exist, it should be possible to improve and combine those techniques in a way that would stop all but the most determined adversaries. Eventually trusted systems could even be made ‘break once break everywhere’ (BOBE) resistant. To achieve this though, the whole industry would need to agree on one standard that in turn needed to be deployed ubiquitously. Still Haber et al. (2003, p.6) claim that “... this would have little effect on piracy.” The reason being that distribution of content via file sharing systems or the “darknet” is very efficient. So it will be enough if some or even just one determined adversary can break the DRM system and release unprotected content to it (Biddle 2002).

Draconian DRM to the rescue?

If the fact that content which is not associated to a license via any means can still be played is identified as the problem, it could be solved by allowing only content with a license to be played at all. This scenario is called draconian DRM (Haber et al. 2003, p.6). In this world any content without a license would by definition be content that was pirated and could therefore be safely dismissed and unauthorized acquisition would be no problem anymore.

To realize this, several conditions would need to be adhered to:

- All stakeholders would have to agree on one DRM system and standardize it.
- A trusted platform would be required to build upon. This could not be a general purpose computer as that would enable the users to have some insight in how the system works internally and therefore help them to circumvent the DRM system.
- A completely new generation of hardware would need to be sold, while at the same time getting customers to throw out all the old stuff, as every device which is capable of playing content without a license could possibly be used to circumvent DRM technology. This change of hardware generations of course includes getting rid of

[7] A preimage attack would enable someone to find an input message that causes a hash function to produce a particular output. (Cryptography Research 2005)

speakers, sound-cards and monitors that are able to play sound and video from all new general purpose PC's.

- A licensing authority would have to be created. This could be done either centralized or decentralized. A centralized authority could be the government, while a decentralized authority could mean that every recording device signs the content it records.
- Every content would need a license. Especially content that is currently in the public domain or where the owners do not even want it to have a worldwide known license. (Think of classified documents or private home or erotic movies)

This clearly is not feasible. While a standardized DRM system seems unlikely at best, selling new computers to customers that are not able to play sound and video will be hard. Remember that at the same time you need to sell them completely new tamper resistant systems just to play sound and video. Also a central licensing authority will have big problems with private or classified content, while we don't even know how a distributed licensing authority could work. We can imagine that every device signs its own content, though this would make it easier to forge licenses. Also if playback wasn't restricted to this device this would only delay the problem by one step, as the recording device would need to reliably distinguish between public, private and copyrighted material.

That means a separate infrastructure for unlicensed content will still be needed, which breaks the whole purpose of draconian DRM.

One could argue that mandatory DRM systems could try to distinguish themselves to customers via lower prices or better features, though I have found no logical argument why vendors of DRM-less systems shouldn't offer those features too.

To sum this all up: There is an argument that says: If we lock the content all up in software, protect the secrets by "gooping them up in Epoxy" (Doctorow 2004) put it into an extra machine and at the same time rip out the ability to play music and video from 'regular' multi purpose computers... Then there is a chance that piracy could in fact effectively be stopped by technical means. This scenario however is so unlikely that protecting against death by falling asteroids could in fact be more productive (Please note the slight sarcasm). Even if this was all sorted out there is still the problem of "fair use" which needs to be allowed.[8]

Accepting Piracy?

As I have shown in the previous parts, piracy of content will remain with us. Business in the era of the internet has to accept that piracy exists and is competing with what they have to offer. On the one hand, this is bad for business as they have to actually deal with the competition from piracy. On the other hand, this may even turn out to be good for the customers as they get better offers out of this.

While of course one cannot predict the future, history has shown that whenever a new technology emerged, that completely changed the way we perceive content –

[8] At least in Europe where the notion of "fair use" is much clearer defined than in the USA.

the overall market enlarged by a big margin. (Lessig 2004, p.53) Of course those who were big business before this change were not the ones to be big afterwards. But the market grew as a whole.

To talk about the current technology: There is no evidence out there that it will not have the same effect on the content creation business. (Lessig 2005) There is also no evidence to show that those who are currently what we consider global players will survive this change in technology as the “big businesses” they are today, but its entirely possible they will. All the while, this of course does not imply that artists or creators will get payed less after this change. Lawrence Lessig for example says that it should easily be possible to model the way we pay creators so that they actually get more money. (Lessig 2005)

To sum it up: Piracy of content is going to compete with those who sell it.

Old perceiving revolutions

The internet is not the first revolution which enlarged the market of content by a considerable amount. Recorded Music, Radio, Film, Cable TV all revolutionized the way we perceive content.

When recorded music became available through Edison's phonograph and Fourneaux's player piano composers and publishers were more than unhappy about the fact that companies sold recordings from their scores without paying them a dime. As the Senator of South Dakota Alfred Kittredge said at that time: "Imagine the injustice of the thing. A composer writes a song or an opera. A publisher buys at great expense the rights to the same and copyrights it. Along come the phonographic companies and companies who cut music rolls and deliberately steal the work of the brain of the composer and publisher without any regard for [their] rights." (Kittredge 1906) The "music publishing industry" was thereby "at the complete mercy of one pirate" (Burkan 1906)

However, the market today is many times larger than it was then.

The cost of fighting piracy

Fighting piracy costs quite a bit of money. First of all DRM systems need to be developed. Then they need to be deployed and after that enforced. Following that, some customers won’t buy the protected content as it is less valuable to them (Biddle et al. 2002. p.15), while some who would have otherwise pirated it will now buy it instead.

This means high costs on the one hand, and hard to predict and even harder to measure gain on the other. But still the cost of introducing and enforcing DRM systems needs to be smaller than the difference between the turnover made from those who would otherwise have pirated the content and those who will now pirate it. Otherwise it would be economically pointless to introduce it.

To sum this up: It is debatable or at least very hard to measure if fighting piracy will pay back.

Is competition with free possible?

While this may seem like an impossibility at a first glance, quite a few businesses actually do it. The most important thing to notice here is that although freely shared content might seem “free as in beer”, users actually have to go to quite some lengths to get content of good quality. So in reality the cost is never “zero” but at least (very) low.

One model to insure that creators get paid in the age of the internet is based on a solution to the free riders problem, which is that a government simply collects an equal amount of money from all its citizens and then spends it on the good in question. This model has come to be known as the "culture flatrate" or "p2p tax".

While this form of compensation is already used in Europe for television and radio royalties, royalties on blank media or even to pay waste disposal, it is quite a new idea for the USA.

This model of compensation is demanded by many entities, for example the Wizards of Oz, CCC, Grüne Jugend, Fairshare, and Attac. (For more information please go to contentflatrate.org)

One business that has many experiences with this is the software industry. Around 40% to 50% of all software is pirated, but the software industry is doing very well. (Haber et al. 2003, p.8)

Another industry that deals very well with free or low-cost competition are the water sellers. The free version of water is of course tap water. It is delivered to your home for a negligible fee, you have the convenience of getting as much as you want from the tap, even if you live on the 10th floor of a building. In contrast, you have to buy mineral water in small quantities, for a (comparatively) very high price. You also have to bring it to your home yourself, especially if you live e.g. on the 4th floor with no lift.

The interesting bit here of course is that neither table nor tap water is superior to the other by any means. Often enough tap water (at least in Germany) is actually better in all respects than bottled water. None the less water companies have a thriving business and will likely continue to do so.

Summary: Competing with free is very much a possibility.

How could competing with “free” work?

There are quite a few advantages that a legal business has over what a pirate could offer. They boil down to basically being legal and using this fact to give guarantees to the user.

1. A business can guarantee great content management in their offerings. It can organize the content in consistent but nevertheless orthogonal categories with a fast and accurate (or even better inaccurate[9]) search engine. All the content can be linked together, so that you can jump from one offering of an artist to all his other offerings or to collaborations he had with other artists or even just to information about the project or the artist himself.

[9] By inaccurate I mean that a typo in the search string still produces good search results, or at least, like Google does, proposes a correction.

2. A business can do much better content delivery than a file sharing network. For example there are no quality control measures in place on the files in peer to peer networks[10], while a business could have them. Also a specific vendor has full control over his offering and can prevent spam in this system, while this may become a big problem in peer to peer networks. For actually downloading the content a vendor can easily ensure that only the capacity of downstream of the customer constrains his download speed. In file sharing networks however it is often the capacity of the uploader that determines the download speed. This is especially interesting as (at least in Europe and much of the USA) the download speed or downstream is typically much higher than the upload speed or upstream of a high speed internet connection. Also a nice offering a business could do is giving the customer cheap and easy access to his files from everywhere. Mobile networks, for example, still are walled gardens. Nobody has access to the networks except the carriers themselves. However, a vendor could strike a deal to give his customers access to their content for a small fee. No pirate could do that.

3. A business can adapt its business model. That is, it can adapt to what people are willing to pay for the content or it can offer alternative ways of charging for the access to its material. Price discrimination[11] is a great tool to extract the maximum of what a customer is willing or able to pay. Students for example could get a discount on the music they buy so they are discouraged from pirating it, as they would probably not have the money to buy it otherwise. On another tangent, business can link its offerings together, for example sell t-shirts with a CD or DVD, bundle concert tickets or a club membership or just plainly and simply do a nice inlet in a CD or provide novel cases made from cloth or cardboard.

To sum this up: This was just a short overview about some simple things that vendors can do to set themselves apart from pirates. If one dares to take a closer look, the possibilities are endless.

Conclusion

In this article I first tried to show how difficult if not impossible it would be to really solve the problem of piracy on a technical level. Even with technologies like the ones that the Trusted Computing Group promotes, it will not be possible to reliably solve this problem by technical means. (Biddle et al. 2002, p.15) The second thing I tried to show were the enormous and very unlikely changes our society would need to endure if a technical solution was tried. From this we have to conclude (Biddle et al. 2002, p.15 and Haber et al. 2003, p.8) that piracy of content will remain and is in fact competing with legal offerings. The ways in which this could happen are what I concluded with and which I'd like to emphasize again: Piracy will proceed to compete with legal offerings however the debate about DRM systems will end. Whether businesses like this fact or not, they have to think about this and react to it in sensible ways.

[10] There are some file-sharing networks that try to build quality-control measures. However, to make them spam-resistant they require user authentication. This though requires a centralized server which can easily be attacked by legal means.

[11] For an explanation of Price Discrimination please see
http://en.wikipedia.org/wiki/Price_discrimination

Outlook

Now it might be that some entities in our society have in fact gained so much influence on our current decision makers that they are able to delay the process of transformation of our society, a transformation to an information society and especially a transformation of how we access and perceive content. But that is a different topic, on which I would advise the interested reader to head to the work of Lawrence Lessig and especially his work concerning the Creative Commons.

Reference

Anderson, James P. 1972. “A Unification of Computer and Network Security Concepts”. IEEE Symposium on Security and Privacy, Vol. 00, p. 77, 1985.

Biddle, P., England, P., Peinado, M. and Willman, B. 2002. The Darknet and the Future of Content Distribution. In Lecture notes in Computer Science, Vol. 2696:155-176. Springer, Berlin

Burkan, Nathan. 1906. In: To Amend and Consolidate the Acts Respecting Copyright: Hearings on S.6330 and H.R.19853 Before the (Joint) Committees on Patents, 59th Cong. 59, 1st sess. (1906) (statement of Nathan Burkan, attorney for the Music Publishers Association)

Jobs, Steve. 2003. Interview with Rolling Stone Magazine. http://www.rollingstone.com/news/story/_/id/5939600 - Inspected 3.7.05

Craver S.A., M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D.S. Wallach, D. Dean, E. Felton. 2001.“Reading between the lines: lessons from the SDMI challenge,” Proceedings of the 10th USENIX Security Symposium, Washington, D.C.

Cryptography Research. 2005. http://www.cryptography.com/cnews/hash.html – Inspected 3.7.05

Doctorow, Cory. 2004. http://www.craphound.com/msftdrm.txt - Inspected 3.7.05

Fraunhofer. 2004. http://www.idmt.fraunhofer.de/eng/projekte_themen/index.htm?audioid - Inspected 3.7.05

Giessmann, Ernst-Günther. 2005. At http://www.informatik.hu-berlin.de/top/lehre/SS05/ringvorlesung/abstracts.html#050616 - Inspected 3.7.05

Haber, S., Horne, B., Pato, J., Sander, T., Tarjan, R.E. 2003. If Piracy is the Problem, is DRM the Answer? In Lecture notes in Computer Science, Vol. 2770:223-233. Springer, Berlin

Kittredge, Alfred. B.. 1906. In: To Amend and Consolidate the Acts Respecting Copyright: Hearings on S.6330 and H.R.19853 Before the (Joint) Committees on Patents, 59th Cong. 59, 1st sess. (1906) (statement of Senator Alfred B. Kittredge, of South Dakota, chairman), reprinted in Legislative History of the 1909 Copyright Act, E.Fulton Brylawski and Abe Goldman, eds. (South Hack- ensack, N.J.: Rothman Reprints,1976).

Kuhlmann, D., Gehring, R. 2003 in DIGITAL RIGHTS MANAGEMENT Technological, Economic, Legal and Political Aspects Springer Verlag, Berlin 2003. LNCS Volume 2770 / 805 pages / ISBN 3-540-40465-1

Lessig, Lawrence. 2004. Free culture, How big media uses technology and the law to lock down culture and control creativity. Penguin Press, New York

Lessig, Lawrence. 2005. The Comedy of the Commons. Podcast: http://www.itconversations.com/shows/detail349.html SD-Forum Distinguished Speakers

Mako Analysis. 2004. Open Device Operating Systems: Opportunity or Threat? http://www.makoanalysis.com/newsletter/example.pdf Mako Analysis, Speen

Relatable. 2003. http://relatable.com/tech/trm.html - Inspected 3.7.05

Stanford Encyclopedia of Philosophy, Free Riders Problem. http://plato.stanford.edu/entries/free-rider/ - Inspected 3.7.05

Stefik, Mark. 1999. "The Internet Edge: Social, Legal, and Technological Challenges for a Networked World". MIT Press. Cambridge, MA & London, UK

Trusted Computing Group (TCG). 2004. TCG Specification Architecture Overview. https://www.trustedcomputinggroup.org/about/faq/ - Inspected 3.7.05

Wikipedia, Psychoacoustics. http://en.wikipedia.org/wiki/Psychoacoustic - Inspected 3.7.05