

Secure Digital Music

Stefaan Motte

Frederic Grumiaux (Philips ITCL)

Frank Piessens

Marc Vauclair (Philips ITCL)

*Report CW309, also published as Philips Technical
Report PLR-13798 , May 2001*



Katholieke Universiteit Leuven
Department of Computer Science

Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

Secure Digital Music

Stefaan Motte

Frederic Grumiaux (Philips ITCL)

Frank Piessens

Marc Vauclair (Philips ITCL)

*Report CW309, also published as Philips Technical
Report PLR-13798 , May 2001*

Department of Computer Science, K.U.Leuven

Abstract

This report discusses the current state of the art of Digital Rights Management (DRM) for digital music files. We define what is expected from a DRM system, what new usage and distribution possibilities it offers for music distributors, and what security technologies can be used for enforcing the DRM system.

Keywords : Digital Rights Management, digital audio, security.

1 The current situation, with all of it's problems

Corporate computer networks are flooded with illegal mp3 audio files, illegal copies of copyrighted music are omnipresent in our youth's cd-collections and schools, not to mention the Internet (just think of the whole napster saga).

These are just a few examples that demonstrate the widespread infiltration of music piracy in everyday life, and perhaps the biggest problem is that almost nobody thinks it's really a problem. Indeed most people find it quite normal to copy music: the price of a simple cd is way too high, they often only contain a couple of songs that are really good, and the music industry makes enough profit anyway. And above all, everybody copies, so why shouldn't you?

All of these are well-known arguments, used frequently by people trying to justify just why music piracy isn't theft. It has also been around quite some time (the same discussion arose when the cassette was launched many decades ago), so one could wonder what's so different about the present situation.

Well, the situation is fundamentally different in relation to a couple of years ago, due to two major factors:

- People are now able to make perfect digital copies, thanks to the low prices and ease of use of cd-recorders and -writers. This is fundamentally different from analogue copies, since these always introduce errors. Digital copies in contrast are a perfect facsimile of the original.
- The problem has taken a global scale. Indeed the advent of the Internet also created a global distribution network for music files. Whereas a decade ago you were always limited to the records that circulated in your circle of friends, nowadays you can literally download any song from anonymous servers. These can be located a few kilometres away, but can just as easily operate from another continent.

At first, this may seem enough to give any CEO in the music business a serious headache, but when you think about it, this really isn't so. Indeed these new technologies bring on a whole lot of new possibilities as far as (legal) music distribution is concerned. These will be presented in the next section.

The real problem indeed is that the music industry lacked to develop an adequate security system, adapted to these new technologies. That, in combination with the fact that the law is not really adapted to the (global) possibilities created by the new technologies, can be considered as the real problem.

Consequently, the answer to the piracy plague does not lie in big lawsuits, but in finding an adequate answer to these two problems: guarantee security through technology, but also create a global legal framework, so that people at least know where they stand (and that big-scale offenders can be punished). Both of these aspects will be handled later on in this text.

2 Digital Rights Management to the rescue!

2.1 Definition

Contrary to what one might think, the new technology is not all bad news, even quite the opposite. If used in the right way, it can indeed be as big a revolution as say the cd and cassette were. But unlike in the days of their release, security now is a big issue, one that can no longer be neglected, as was the case for years.

Indeed, billions of Euro in profit are missed out on every year because of piracy, so a system that guarantees that people who should get paid, actually do get paid is more than needed. And in comes *Digital Rights Management* (DRM)!

The whole purpose of DRM is indeed to:

- guarantee that copyright rules are respected. This means that playback or copying of a song should only be permitted to people who have that right (e.g. who have made all the proper payments). This security has to hold at all times: during the storage on the central server and on the customer's devices, but also during all transport.
- add certain *usage rules* to the musical content, and act accordingly. These rules exactly state what is, and what is not permitted. For a classical cd for example such a usage rule is that it can be played by anyone, and copied by no one. From now on, much more refined rules can be specified, including limitations on time, duration, quantity, ...
- take care of all the financial aspects. This means that the system must make sure that the money flows correctly from the consumer to the provider, the producer, the author...
- make this whole process transparent to the consumer. From his point of view, digital distribution should be as easy as walking to the music store. Requiring him to go through a complex sequence just to buy or even play a song is certainly not an option.

All of this comes on top of providing the actual music. Indeed the customer has to be able to acquire music through digital distribution, yet his current music collection should remain usable on the new technology.

That realising all of this is not easy should be clear. If indeed it was, performant and reliable systems would already exist, alas they don't. Security is the big problem, as is to be expected. Not only does the research on the topic just begin to mature, but full-proof security often conflicts with usability and transparency to the user. Since those two criteria are an absolute requirement for many CE applications, a compromise will have to be made.

Indeed absolute security is no longer the primary goal. DRM Systems aim to "keep the honest people honest". What this nifty slogan means, is that it should be made hard to crack the security system (thus discouraging the amateur or casual hacker), but not to such a point that the system becomes inoperable. Professional crackers with specialised equipment and a lot of time will probably be able to crack the system and copy some songs, but so be it. It's up to the law to deal with such cases.

The whole point is to avoid the current situation where any 14-year-old with a multimedia computer can begin copying and selling cd's. Professional piracy on the other hand is a whole other thing, and does not fall under the responsibility of current DRM Systems.

Of course security breaches have to be kept local, meaning that they mustn't compromise the entire system's security. A situation where for example (professional) crackers could devise (be it at great expense of money and time) and distribute a program on the Internet, permitting the above-mentioned 14-year-old to restart copying is of course not permissible.

2.2 *New possibilities*

Once all of the necessary security measures in place, we can finally explore the new possibilities of digital distribution. These can roughly be classified in two categories: *usage* and *distribution*. We will examine both of them below.

2.2.1 Usage

As mentioned when summarising the functions of Digital Rights Management, far more detailed usage rules can now be embedded within a song. These rules may grant the consumer certain right for:

Copying: Examples are:

- *Copy never:* no copy is allowed
- *copy x times:* x copies of the original are permitted. Once that number is reached, no more copies are possible
- *copy once:* the user can make copies of the original, but the copies cannot be copied further
- *copy freely:* the track can be copied without any problem. The same applies to copies of the original and this to any depth.
- *Number of local copies:* a user for example might get the right to have a maximum of x local copies at all time (e.g. one in his computer, one in a portable device, ...). Through a sort of check-in/check-out system local copies can travel from one device to another, while some local device is responsible to uphold the constraint that no more that x copies may exist simultaneously.

Listening: With the classical media such as a cd, once a consumer buys the product, he can listen to it forever, without restrictions. Thanks to DRM, this can be brought a step further. A person can now buy a *listening licence* granting him the right to:

- *Listen freely:* this is comparable to the existing situation with cd's.
- *Listen x times:* one buys or gets the right to listen a fixed number of times to a song. Once this number is reached, the song becomes unusable, unless a new licence is purchased. Note that this system is also ideal for promotions, where a music company *gives* the user the right to listen once or twice to a song (of course hoping that he will buy

- a license afterwards).
- *Listen during period*: The consumer buys the right to listen to the song during a fixed period (a day, a week, ...). This could come in handy for occasional dj's. Thanks to this system, he could always have the latest music on hand, without having to buy it all. He would just have to get a licence for those nights he plays (which hopefully should turn out to be cheaper)
 - *Time-shifted listening*: This means that the content can be listened to for a given amount of time after recording. Although similar to the previous point, its use is different. Imagine for example digital radio. Recording a program and listening to it at a later time is of course already possible. Now, we can limit that time. One could for example state that a program can only be listened to within a week after broadcast, and thus prohibit the listener to create his own permanent archive. The same applies to streaming audio on the internet, where you could permit local buffers or proxies, but limited in time
 - *Pay-per-listening*: With this system, the user does not have to buy any separate licences. He can listen to what he wants (the entire company music catalogue). His intelligent audio system keeps track of what was listened to, and at given times (e.g. once a month) presents the user with a bill to pay. This is probably the most transparent and easy system as far as the consumer is concerned.

Location: In contrast with a cd, music is no longer tied to a physical medium. This means that the rights corresponding to that song also don't necessarily have to be tied to a physical entity. Indeed, the rights can be tied to:

- *The song*: in this case, the song can be moved from one device to another, and the rights can be used by anyone.
- *The device*: the device is granted the right to perform certain actions on certain songs. In this case, a songs remains tied to a single device
- *a person*: it is now the responsibility of a device to control the identity of a user, and the rights he has. Only operations on songs conform to those rights are permitted. This identity and rights can for example be stored on a smartcard, but also on a central server. All the user would then have to do is authenticate himself to that server. All of his rights could then be temporarily downloaded to the device

All of these approaches have pro's and con's. The first one is certainly the most *natural*, while the second one is quite *easy* to implement. The third is probably the most interesting. This system indeed permits listening to *your* music anywhere you want (either by providing your listening rights trough a smartcard or by downloading them), *without* having to provide the audio itself. The songs can be downloaded (from a central or local server) to the device when needed.

2.2.2 Distribution

By this we don't mean getting the song from producer to consumer, but the possibilities such a consumer has to further (re-) distribute the song or licences he bought. Since cd's are a physical thing, they can be sold, lend, given, ... Listening rights as used by DRM Systems on the other hand are pretty intangible, so all of these operations (if wanted) have to be explicitly put into the model. These include:

- The right to *sell a song/licence* to another person. Depending on the licensing model used, this may require the intervention of a central system, maintained by the content provider. Especially in the US, where the right to sell is considered part of *fair use*, this right to sell may not be overlooked.
- The right to *lend a song* for a certain period to someone else. This comes down to temporary transferring your rights to another person. After the period passes, everything automatically returns to normal.
- *Superdistribution*. This is particularly interesting for the music business. It assumes that people will send songs they like to their friends (e.g. by e-mail). This friend could then (automatically) be granted the right to listen to it once or twice. The idea is that, if he likes it he will then obtain a licence for himself. The beauty is that there was no work or advertisement necessary from the music business. The song truly sells itself.

3 Security components, common to many contemporary DRM Systems

3.1 The building blocks

Although the research on audio protection is still ongoing, and thus several, sometimes conflicting, theories exist, most DRM Systems make use of the same major principles:

1. The content must be protected at all times.

This involves two things:

- the storage within the device must be secure
- the content may not be *readable* to eavesdroppers during transfer from one device to another. This will probably come down to scrambling it in some way.

2. Communication can only take place between trustworthy devices

To see that this is indeed needed, consider a *trustworthy* application communicating with a non-trustworthy soundcard. Although all the security measures may have been taken up to the soundcard (including secure transfer), this soundcard can essentially do whatever it wants with it's copy of the audio, including making an illegal copy.

So it is essential that digital content only travels from and to devices that are considered/proven trustworthy.

3. The usage rules must be inseparably and inalterably connected to the audio content

If this were not the case, it would be easy for hackers to isolate and replace these rules with self-constructed ones. It is conceivable that, just by experimenting, they would ultimately find a combination that gives them all the rights they need.

This can be circumvented by adding the information to the content in such a way that it can not be directly altered by unqualified people (e.g. who don't have the proper key) without also altering the content..

Another option is to actively search for such alterations, and deny the content if such *tampering* has been detected.

3.2 What's needed?

These building blocks of course have to be translated into actual techniques providing the wanted result. Although this sometimes will be pretty straightforward, in other cases it will strongly suffer from the immaturity of the needed technology. As could be suspected cryptography will occupy a central spot in this all.

Following techniques are commonly used:

1. Encryption

Encryption has proven its merits over the years, and it's an almost natural choice as far as secure storage and transfer are concerned. When using a relatively secure and well-tested algorithm (such as TEA, RIJNDAEL, DES, ...), and a secret key of sufficient length, this part of the security architecture may be considered secure.

To generate such keys (for example between two devices wanting to engage in communication), well-reputed cryptographic algorithms such as Diffie-Hellman can be used.

2. Authentication

Like we pointed out before, it is absolutely necessary that both devices wanting to communicate can authenticate one another (to be assured of the other device's trustworthiness). Two different approaches can be taken:

- *Shared secrets*: When both devices are equipped with one or more shared secrets (secrets that are only issued to trustworthy devices), the authentication can be realised by some sort of challenge-response protocol using this secret. It is however essential that those secrets are never exposed on an insecure line, since this would compromise the entire system's security
- *Digital Signatures and Certificates*: Also well known in the cryptographic community, these roughly perform the same task as their real life equivalents. By using a Digital signature (which can be verified through a certificate issued by a trusted third party), a device can prove its identity.

3. Watermarking

This is without any doubt the least mature, and probably least known of the here proposed techniques. Basically it embeds information into something else (music in our case), in such a way that it doesn't noticeably alter the content.

Two different kinds of watermarks exist. The first kind, called *strong watermarks*, can't be removed or changed (without the proper key) without changing the content.

This is in other words exactly what we are looking for to attach our usage rules to the actual musical content.

The second kind are designed in such a way that they withstand certain operations, but disappear when other, specific transformations are applied. They are called *weak watermarks*, and have to be specifically designed in function of the manipulations one wishes to detect.

If such a watermark was embedded, and we want to make sure the corresponding operations were not applied to the content (e.g. operations that would disable the main protection system), all we have to do is check if the watermark is still present. If not, the content has been tampered with.

Although pretty efficient watermarking schemes exist for video and still images, this is not the case for audio. There surely exist algorithms matching some of the requirements (such as robustness, inaudibility, data rate, ...), but one that fulfils all of the requirements has not yet been proposed. This is due to several factors, such as the performance of the human hearing, the limited bandwidth in audio (especially when compared to video), the performance of the current codecs, ...

Since many DRM Systems do rely on watermarks, this of course poses a serious problem. That is why current systems should only be considered as an intermediate result, just a step in the ongoing research.

3.3 How does it all add up

Although sometimes other security measures are added, the above mentioned components often form the core of a protection system. Schematically, when two devices want to exchange content, the following procedure is followed:

1. Both devices authenticate each other
2. A common secure session key is generated by both devices
3. The content is encrypted at one end using this key, and then sent to the receiver. There the content is decrypted using the same key
4. The receiver now checks whether the weak watermark is present, if not, the content is rejected
5. The strong watermark is analysed, and the usage rules are retrieved. The receiver now acts accordingly to these rules.

One example of a system wanting to use this kind of protection system is the SDMI, which we will look at in the next section.

4 SDMI: DRM in practice... or not?

4.1 The context

Although these building blocks and even explicit techniques are commonly used in many of the contemporary DRM Systems, this does not mean there exists some sort of uniformity between those systems. Indeed many of them differ on things like (the location of) licence management, possible usage rules, security level, ... This often results in mutually incompatible file formats.

The consumer from his part is of course not willing to buy a product that's still in a state of (r)evolution. Indeed a DRM System can be obsolete in a matter of months, and if the device you bought only supports one native format, you've suddenly got a pretty expensive useless thing in your hands

This can somewhat be solved by incorporating several formats and systems into one CE device, and providing extensive upgrade capabilities. Although this last option certainly is a must, the first one can't always be accomplished. Current CE devices are indeed characterised by very limited processing and memory resources, possibly not allowing several formats to co-exist.

Luckily the industry realised something had to be done, thus creating the SDMI.

4.2 The goals

The SDMI, which stands for Secure Digital Music Initiative, is an industry wide consortium, with members ranging from mobile phone-companies over hifi-manufacturers to record labels. If a company has anything to do with audio, it's probably represented.

The main goal of the SDMI is to develop a standard as far as DRM is concerned. This certainly does not mean that if the SDMI succeeds, there will only be one product available with different labels on it. They just want to generate a framework, which the individual companies can build a product on. This framework will offer guarantees towards consumer on things like security, compatibility, upgrades, ...

The only intention of this framework is to formulate a list of requirements all sdmi-compliant devices must meet. It's then up to the individual companies to come up with an actual system that meets these requirements (in order to obtain the "SDMI-Compliant"-label). The choice of individual algorithms and techniques still remains the responsibility of these companies.

One exception on this rule exists though, and that is with regard to the watermark. Indeed the SDMI protection system uses watermarks (strong and weak). Since this can be considered one of the core elements of the security mechanism, it seems necessary to impose one specific watermark (also for compatibility reasons). Another, more reality-driven reason is that audio watermarking technology hasn't fully matured yet. One of the goals of the SDMI was to find such a watermark that fulfilled all requirements. As we shall see shortly they did not succeed (yet).

4.3 The provided functionality

The SDMI knew that such a framework could hardly be designed overnight, especially with the current state of the needed technology in mind. This explains why they've opted for a 2-

phase design. The first phase offers very little security and functionality, and should only be considered as an appetiser and grand-rehearsal for phase 2.

We will quickly go over the functionality offered by each phase:

- **Phase 1:**
 - limited copy control through CCI-bits.
 - detection of phase 2 trigger. When this trigger is detected in the content, the user is prompted to upgrade his software to phase 2. If he does not, the device continues to work, but will not render any content that contains this trigger.
 - several (4) local copies are allowed. These can move from one device to another through a move-in/move-out system.
 - a local SDMI domain. This domain is deemed secure, and all content must first be imported into this domain in order to be rendered. During this import, the validity (against playback and copy rules) of the content will be checked.
 - playback: all current formats such as wav, mp3, cda, ... can be imported and played.

- **Phase 2:**
 - major improvements on the security system (the aim is to actually make it work). The security system will use a strong watermark to embed the usage rules, a weak watermark to detect tampering, a system that checks the presence of the entire cd (if applicable), ...
 - far more detailed usage rules

As you can see, the SDMI primarily focuses on security. Nothing keeps the individual companies from adding more functionality on top of that. The design of phase 2 should have been done by January 2001, in order to have the corresponding devices in the shops by Christmas 2001. Alas, as we shall see in the next section, this goal was not achieved.

4.4 Anything but a blue sky

Although the press releases from the SDMI present a somewhat different tale, not all is well with the SDMI. Specifically the watermarks suffer from serious problems. Since these watermarks can be considered as the heart of the entire protection system, this jeopardises the entire project.

4.4.1 The hack SDMI contest

Just as with phase 1, the SDMI opted to launch a public contest in order to choose the phase 2 (watermark) technology (although some people suggest that it was all one big masquerade, and that the Verance watermark had already won before the contest began). Anybody could propose a watermarking scheme, as long as it satisfied certain requirements. One of these requirements was that, if chosen, the watermark could be used free of charge by the SDMI.

After a first screening of these contenders by the SDMI, a second challenge was issued, this time to break the proposed watermarking schemes. This (once again public) contest, known as

Hack SDMI, promised up to \$10.000 to anyone who managed to break (or find flaws in) one of the watermarks.

More concretely, some PCM files with embedded watermark were made public, and it was up to the hackers to remove this watermark (in a *repeatable* manner). The quality of the music after this watermark was removed had to be equivalent to, or better than mp3 at 64 kbps.

Contrary to many press releases, the contest that ended in October 2000, was not a success as far as cracks are concerned. That is, only one watermark had been successfully hacked. This of course looked very promising, since it suggested the other watermarks were *good*.

Yet we should question these results. Indeed some researchers claim to have broken all the watermarks. In "Reading Between the Lines: Lessons from the SDMI Challenge", available at <http://cryptome.org/sdmi-attack.htm>, such "successful" hacks are described. Although they were initially accepted by the SDMI, they were finally rejected based on some degradation of the music.

From these test, quite some information concerning the watermarks was won. For instance, they discovered that the Verance watermark (which will probably be pronounced the winner, remember) used some kind of complex echo hiding scheme, with multiple time varying echo's.

The SDMI immediately started threatening with legal actions, based on the Digital Millennium Copyright Act. Under this law it is indeed prohibited to tamper with copy-protection systems, even for academic research purposes. This once again shows the danger of this law, since it could destroy all future academic research on the subject

Luckily the researchers didn't comply, and published anyway. They deserve our utmost admiration for this.

One should of course make several reflections on such contests. It is not unimaginable that someone who did manage to break a watermark would keep this quiet. This watermark could well become the heart of *the* music industry's security system. If one possesses the *key* to crack this system, much more money can be made. We leave this reflection for what it is.

4.4.2 Tests made by the SDMI

Of course the hack SDMI contest was not the only means of testing that was used. The SDMI itself also ordered some tests, such as robustness tests, audibility tests with so-called "golden ears" and analytic attack tests.

The "*golden ears*"-tests proved very successful. Most of the watermarks were effectively inaudible. In November 2000 3 candidates remained, each of them meeting all the requirements so far.

But the *robustness tests* were a less encouraging. These were carried out in certified labs, and included looking at the reaction of the watermarks on common user DSP operations such as bass, treble, sample rate conversion, time scale change, dynamic bass boost, AAC compression,

MP3 compression, D/A->A/D, Not all of them at the same time, but some combinations were tested.

The aim of these tests was to check if the watermark and its payload were correctly detected after the music had been exposed to all these kinds of bad consumer treatments. They also examined if a watermark was detected while there was none embedded.

These results were not that positive. Indeed no proposed watermark really passed these tests. This means that in some cases the system could detect a watermark when it's not present, and in other cases not detect it when it is present. This just by applying such operations.

The first problem is bad, but the second one is even worse. Indeed it is not permissible that someone who legitimately bought a song, is not able to play it. Forbidding common operations is also not an option.

Finally *analytic attack testing* was done. This came down to having people who were specialised in cryptography and watermarking analyse the remaining watermarks. To do this, they received detailed information on, and the explicit algorithms of these watermarks.

These took quite some time, primarily because it was hard to find such *experts*. Not that they don't exist, but most of them work in (competing) firms. Given the sensitive nature of the research, this was not really an option. But also in the academic world such people proved hard to find.

4.4.3 Maybe not just yet

The bad results of all these tests (robustness tests in particular) were of course a major setback for the CE industry, which wanted fully functional phase 2-devices in the shops by Christmas 2001.

Given the bad state of watermark technology, some decisions had to be made: continue with watermarking (and hope for a short-term breakthrough), or find something completely different.

Although around January 2001 most people were expecting that watermarks would be dismissed for the time being, this eventually was not the case. Indeed during spring 2001, some (but not major) improvements were made, and the SDMI deemed these revised watermarks *sane* enough to be used.

Around July 2001 the complete specifications for phase 2 should be available, and these will include a watermark. At the time of writing (April 2001) three watermarks are still in the running, being Verance, CRL and Blue Spike. Like we already said, Verance will probably turn out to be the winner.

Together with this watermark, another safety mechanism will be included. This mechanism will ensure that (when applicable) the complete cd is present when a song is played. If the cd is not detected, playback will fail. The two major contenders in that department are Philips and EMI. They roughly do the same, but in a completely different manner.

4.5 So what about the future

As can be suspected, phase 2 will be nothing more than yet another transition phase. The watermarking scheme is not as mature as it should be, and honestly speaking the SDMI has somewhat lost its credibility for many companies.

One of the reasons for this sudden loss of faith is that the SDMI set July 2001 as an absolute deadline for the specs of phase 2 technology. For one thing this has caused the to be released *standard* to be immature, and probably not very safe. And sure you might argue that this date was chosen to keep the engine of economy turning (and get *new* devices in the shops by Christmas), but even this is questionable.

Indeed the companies who develop software players (such as real audio player) have new releases every three months or so anyway. For hardware manufacturers this date is just too late. In order to have fully functional and tested devices in the shop by Christmas, while only getting the specs by July, companies would have to invest tremendous amounts of effort and money.

Bearing in mind that phase 2 isn't all that good, companies will surely have some doubts before engaging in this costly adventure.

4.6 Conclusion

The least thing we can say is that the stars SDMI was born under aren't really favourable. The goal of developing a secure and flexible DRM framework is hard as it is, but having to cope with the lobbying of the more than 180 companies that populate the SDMI may be even harder.

Not only do they all want to favour their own native technology, but the demands they make often point in different directions. The record labels want a working, fairly safe and highly functional system yesterday, the CE industry just want to have a product in the shops by Christmas, and the IT sector wants to slow the whole thing down.

Indeed from an IT point of view, all of this is considered cumbersome, since all of the laws and rules on music copyrights mostly apply on pure audio devices (which computer's aren't considered to be).

Coping with all of this is hard as it is, so when on top of this all the watermark technology (the core of the entire system) fails, disaster is the only word that comes to mind.

Still we have to give the SDMI some credit, since its goal to bring unity in an industry where there is none is more than necessary. And that any attempt to achieve this goal will bring many problems and chaos with it is nothing more than normal.

So on short term, don't expect too much from the products that originate from the SDMI. They are indeed necessary, but soon-to-be obsolete try-outs, just teasers until the real stuff is developed and released.

This does not mean that we should ignore the SDMI for the time being, even quite the opposite. The SDMI remains an interesting concept, from which the future DRM standard

may evolve. Or, just as probable, it may turn out to be the flop of the century, a lot of fuss about nothing.

Nobody really knows, and that is probably why everybody keeps on looking...

5 But what about the law?

As mentioned before, current DRM Systems are not designed to offer full-proof protection. They just intend to make cracking the system as hard as possible, thus discouraging all but the most perseverant (and well-equipped) "pirats". It's then up to the law to take care of this *elite* group.

In this section we will take a look at that law, and see if it's quite up to the task. We will also examine just how illegal home-recording is, and this in several countries.

5.1 *The situation in your typical Western country*

Most of these countries have a law on Intellectual Property that is based on several international treaties, such as the Berner Convention (1971), the Convention of Rome (1961), the TRIP agreement (approved in 1994). We have to note that although many countries do uphold the principles of these conventions, and have officially approved them, not all of these principles were also ratified in national legislature.

The ground principle is that the actual owner of the Intellectual property (the artist/producer in our case) basically has the sole right of reproduction. This means that for every reproduction his approval is needed.

Based on this, any form of home recording of (even if you own the original) copyrighted material is thus illegal. Indeed for every single copy, a written permission of the copyright holder is needed.

Since the legislator well knows that checking all of this is practically infeasible, luckily for us a very important exception was added to the law:

The request for a copy that is purely intended for private use within your family circle is automatically granted. No explicit approval from the copyright owner is needed.

Of course this copyright owner would still like to be paid for each such copy. To accommodate this, a small percentage of the price you pay when you buy a device or media that's capable of making such recordings automatically goes to the copyright owners. To give an idea, in Belgium 0.125 Euro per hour is imposed digital media such as cd's.

This toll by the way does not apply to computers and such, since their primary goal is not considered to be audio copying. Since multimedia computers seem to be the main tool for small-scale copying nowadays, this rule may well be up for revision in our opinion.

We should also note that these laws were all designed with physical media in mind. They are definitely unable to cope with the new situation with digital transmission and distribution.

Questions like what to do with local caches, several copies during transmission, back-ups, ... are not answered.

Initiatives like the Digital Millennium Copyright Act try to overcome this, but not everybody seems to be happy with the result. Indeed they tend to be too restrictive (forbidding *all* copies, including above-mentioned copies during transport). In all senses they give too much power back to the music industry. Based on the protest of many, this will certainly not be the end of the story, merely the begin.

5.2 *A less comfortable position*

Although they often complain, the music industry still occupies a pretty comfortable position in our western world as far as the law goes. Indeed the legal protection may not be ideal, it still goes up to a reasonable point.

Indeed we can imagine some countries where such legal framework does not exist (or is not as protective). This is of course a problem, since the Internet (being the main distribution network for audio pirates) is a global thing. A server may just as easily be set up in a country lacking a copyright law. If this is done, no legal action can be taken against the pirates themselves, only against the individual downloaders (if their country's law permits, that is).

Since this is just the thing we want to avoid (remember that we only want to target organised piracy), the need for a global uniform legal framework should be obvious. Initiatives towards such a framework are indeed on their way (examples are efforts made by the WIPO), but things go slow. When we look at the *speed* at which for example the European Parliament works, this should hardly be a surprise.

To illustrate that such *lawless* countries needn't always be sought in parts of uncivilised Africa, we will briefly discuss the situation in Japan.

Like many countries Japan also follows the Berner Convention and WIPO treaties. Amongst other things, this implies that also in Japan it is the copyright owner that has the exclusive right to authorise copies of his work. In principle that is, because they also introduced a couple of exceptions that, in this context, have grave implications:

- In Japan, any individual has the right to make a copy of music recordings, as long as it is for his personal use, and that he doesn't make any profit from it
- Second, such recordings may be lent, broadcast or communicated, again if no profit is made.

This last exception authorises individuals to set up servers hosting a huge collection of for example mp3-files, and to make these publicly accessible. The first exception authorises people to download files from this server.

This means that neither party is punishable, as long as no profit is made along the way. Since Asia is a huge market, with a flourishing music industry, it should be clear that this situation somewhat worries record labels.

5.3 Conclusion

In its fights against music piracy, the law fails on three major points:

1. It's not adapted to the current technology. As we demonstrated the concept of Intellectual Property is present, even in the context of music, but it's totally oriented towards the classic physical media. Although efforts are made to adapt it to the new digital distribution forms, there is still quite some way to go.
2. Although there is quite some uniformity in the western world, the Intellectual Property law is far from being globally uniform. As the music distribution has become global, a quick globalisation of the law should be considered an absolute priority. Once again, they're working on it, but where making changes to national legislature is slow, making them to international legislation is even slower.
3. PR. Many people simply don't know what is, and what is not permitted as far as copyright is concerned. Just ask someone the question is home recording is permitted, and you'll see my point. The thing is that copyright companies (like SABAM in Belgium) are quick to threaten with lawsuits against violation, but nobody really takes the time to instruct people what is, and what is not permitted. Since one of the primary goals of the music industry is to achieve a general mentality change towards copying, a little information surely isn't too much to ask. Yet they remain silent...

But we mustn't be too harsh, efforts are indeed being made, and even Rome wasn't built in one day. It is a good thing though that they realise something has to change. Now it's just a question of putting these good intentions into practice.

6 Conclusions

As should be clear by this text, DRM is a domain that still is in (fast) evolution. Unfortunately, the research doesn't have the luxury to mature for some years, far away from the (critical) public eye. Due to the nature of the beast, and the absolute need for a music protection system (anything is better than the current situation where there is a total lack of control), every intermediary result has to be immediately implemented in real-life products, often without the proper testing.

Good examples of this are the Microsoft Windows Media Rights Manager, which was cracked just a day after its launch, but also the SDMI. The SDMI indeed constructed its whole security system on the belief a good watermark would be found before the deadline. As it turned out, current watermarking technology isn't quite up to the task, hence the gigantic chaos within the SMI right now.

So I wouldn't bet on seeing a full-fledged, totally safe DRM System any time soon, but it would be foolish to think they're not the future. Between this and a few years it is my belief that DRM will be integrated in every audio device and application, even to such a point that we will begin wondering how we ever did without them.

That day however has still not arrived, and all the current products should only be viewed as tokens of the current stage of research. In a world where scientific research doesn't get the time any more to become adult before it is thrown in the big mean adult world, the fact that

most systems have come so far in so little time is a merit by itself. And it certainly makes you wonder about what's to come.