INDICARE Monitor

About Consumer and User Issues of Digital Rights Management Solutions

www.indicare.org ISSN 1614-287X

INDICARE Monitor Vol. 2, No 12, 24 February 2006

Content

Focus theme: Trust, DRM, and TC

The **IN**formed **DI**alogue about **C**onsumer **A**cceptability of D**R**M Solutions in **E**urope

Editorial of INDICARE Monitor Vol. 2, No 12, 24 February 2006

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The current issue contains 15 articles: the first and the second are appetizers for new INDICARE documents (second survey and fifth workshop). Four excellent articles deal with contracts, copyright confusion, court decisions, and the copyright reform in France. We also report about the DRM session of a recent OECD conference on the digital economy, and review an empirical study which tested the privacy conformance and user-friendliness of DRM systems. The focus theme "Trust, DRM, and TC" is approached in six different ways – among them the ambitious approach of OpenTC, a large project funded by the European Commission.

Keywords: editorial – INDICARE

Two new INDICARE documents published

INDICARE proudly presents the findings of its second European consumer survey. While the first focussed on music consumption, this one is about European Internet users consuming *digital video content*. The article by *Nicole Dufft* of INDICARE Partner Berlecon Research – responsible for the survey – summarizes the main findings. It shows that digital video content is becoming popular in Europe. We learn about consumers' usage habits and expectations, about their willingness to pay for usage rights and their awareness of DRM. The complete survey results are available for free (Dufft et al. 2006).

Kristòf Kerényi, SEARCH Laboratory, organizer of the fifth INDICARE workshop on “Human Factors of DRM” summarizes what he personally found the most interesting facts and conclusions. He especially highlights the session about accessibility for the blind, and the presentations from consumer initiatives. The official report of the workshop, which took place in Budapest on 19 January 2006, will be available from the INDICARE Website in March 2006.

More about the present issue

Contracts, copyright, and courts

Lars Grøndal, a legal advisor for the Consumer Council of Norway, currently working for BEUC (The European Consumers’ Organisation), digs into the contractual terms consumers often accept without being aware of the content. The focus is on contract terms with respect to DRM in the field of online music. The "Terms of Service" (ToS) of iTunes are taken as an example. The article reveals that these ToS contain unfair terms not conforming with the law. In Norway, the Consumer Council has therefore complained to the Consumer Ombudsman in order to get iTunes terms amended. However, as Grøndal makes clear from the beginning, his article is not primarily about iTunes. The type of unfair terms identified is not unique to iTunes, indicating a more general problem in online markets for digital goods and thus constituting a public policy issue.

Matthias Spielkamp, iRights.info, starts from the assumption that the implementation of the EUCD confuses consumers and has made copyright an enigma for laypersons. This point is demonstrated impressively by a case study looking at file-sharing in the light of corresponding legislation in Germany. His conclusion is that publicly funded, impartial consumer information is needed as rights holders can not be expected to provide it. iRights.info, funded by the Ministry for Consumer Protection in Germany, is of course an initiative he has in mind. Beyond the national level he sees a need for multi-national, multi-language efforts at the EU level.

Natali Helberger, IViR, INDICARE's most eloquent legal expert has already been watching developments in France for a while. This time she contributes two closely related pieces of legal analysis.

The first article discusses the latest court decision in France with respect to private copying of protected content: *Christophe R. vs Warner Music*. The court concluded that TPM has to respect the private copying exception. This case underlines that until now, courts had to deal with consumers' complaints about copy-protected CDs or DVDs, while the legislator hesitated to implement the EUCD

And that's exactly the subject of Helberger's second article *Vive la Balance! Pleading for a French revolution of copyright*. The French Parliament launched "Le Project de Loi N° 1206" in order to bring about the long-pending implementation of the EUCD, including, of course, the provisions about TPM.

The analysis of the draft shows Natali's disappointment. Given the vivid public debate about DRM and consumers, and the recent court decisions, the drafted law falls short of expectations. To hold DRM *users* liable for compliance with the law is regarded as a step in the right direction. She criticises, however, that such obligation is of little value without accompanying measures that guarantee its enforcement

By the way, despite the title, Natali is not really pleading for a new revolution. "Creating the conditions for a more consumer-friendly DRM environment is not revolutionary…" she says. But sometimes a necessary reform in a difficult environment against the mainstream might be worth being called a revolution anyway.

Alternative models for content distribution
Daniel A. Nagy, developer of the ePointSystem, working with INDICARE partner SEARCH, comes up with an interesting content distribution framework. The proposed framework relies on peer-to-peer digital payment. It aims at unprotected content, however DRM techniques can aid the business models to become more efficient by reducing transaction costs, e.g. reducing the load on the operators or helping to exclude free-riders. In these scenarios, users of DRM-enabled devices, i.e. consumers, have no incentive to attack DRM systems.

OECD conference report
Philipp Bohn, Berlecon Research, reports about the Future Digital Economy conference, Rome, 30 and 31 January 2006, which was organized by the OECD and the Italian Minister of Innovation and Technology. More precisely he summarizes what was said about DRM at the conference, and in particular during a panel session addressing “Content diffusion: IPR, DRM, licensing, content security, standards”.

Review of privacy4DRM
Knud Böhle, ITAS, reviews a study sponsored by the German Ministry for Education and Research (BMBF). *Privay4DRM* appears to be a noteworthy contribution to conformance testing of DRM systems with respect to privacy and data protection provisions. The scrutiny of data flows and data traces when using DRM systems reveals significant shortcomings. The authors propose to improve the situation by more transparency, end-user involvement, pseudonymity options, and "privacy labels".

Focus theme: Trust, DRM and TC

Mark Bide, Senior Consultant, Rightscom Limited, holds that "informed consumers should welcome the implementation of effective DRM – if it meets their needs". This article can be read as a kind of introduction to the focus theme as it opens up the broader perspective. The general message is that we must think in terms of “network citizenship”, which includes as a major task managing trust on the network. The core concept he introduces is “Digital Policy Management”, a concept which allows for combinations of trust, good will, law and technical protection measures. "Consumers", he says, "will welcome the introduction of digital policy management technology … only if it also offers a solution to *their* underlying security and identity problems and contributes to the maintenance of civil society on the network, with all the complex checks and balances that this implies."

Robert A. Gehring, member of the research group for Computers & Society at the Technical University of Berlin, explains – as precisely as possible within a short article – the relationship between trusted computing (TC) systems and digital rights management (DRM). In his view TC components are tools – in themselves neither good nor bad – which can be used to build DRM systems or to protect "darknets". He warns that strong DRM systems based on TC do not *per se* guarantee successful business models if consumer expectations are not met.

The next article by *Dirk Kuhlmann*, Hewlett Packard Laboratories, Bristol, describes a new Integrated Project (IP) funded by the European Commission, called OpenTC. Kuhlmann has the overall technical lead for the OpenTC project. OpenTC aims to combine TC technology and FOSS and to demonstrate advantages of this approach. The author is convinced that enhanced protection and security based on TCG technology will become standard, and that professional users of non-proprietary operating systems (like Linux) and software will ask for comparable protection mechanisms – independent of whether FOSS communities like it or not. OpenTC aims to fill this gap. Furthermore it claims that the combination of TC and FOSS will have advantages in terms of privacy, efficiency, openness, and consequently user acceptance. The author is fully aware that a lively public discussion is going on about TC, and about the possible combination of TC and FOSS.

Florian Schreiner, *Michael Pramateftakis* and *Oliver Welter*, computer scientists from Munich University of Technology, are partners in the OpenTC project aiming to create a DRM system which governs the use of all kinds of sensitive data from the medical sector to entertainment. The system proposed differs from others, because it will be open-source and will use the TPM-Chip to enforce security. Advantages expected are: interoperability with other DRM Systems, transparency, convenience for users, and support of legacy software

Gergely Tóth, SEARCH Laboratory, writes about the next version of the Symbian operating system for mobile phones, which incorporates Trusted Computing based security features. Mobile phones using the Symbian v9.1 operating system will probably be used for DRM-based applications. Multi-media phones like Nokia N91 and the Sony Ericsson W950i said to implement the Symbian operating system and provided with a 4 GB internal hard disk obviously point in that direction of mobile phones able play and to handle protected digital music.

Last not least *Arnd Weber*, ITAS, Karlsruhe, and his brother *Dirk A. Weber*, an IT-Consultant, have reviewed recent works by legal scholar *Stefan Bechtold* dealing with the risks of trusted computing from a regulatory point of view. The reviewers present Bechtold's arguments and his general view that there are possibly many risks involved, but that they could be handled by skilful design of TC-architectures and proper institutional arrangements. The main threats identified are: dominance of players, lack of capabilities to deal with copyright exceptions, and loss of privacy.

The reviewers however not only summarize the risks and remedies mentioned by Bechtold, but also critically remark that Bechtold might be overoptimistic as he seems to assume that all the hard- and software built on TCG-principles will work properly. This, however, may not be the case.

Sources

- ► Dufft, Nicole, et al. (2006): Digital Video Usage and DRM – Results from a European Consumer Survey, Berlin, February 2006; online available at: http://www.indicare.org/tiki-download_file.php?fileId=170

About the author: Knud Böhle is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 06/03/06; licensed under Creative Commons; included in the INDICARE Monitor, Vol. 2, Number 12, February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=187

Digital video usage and DRM: Results from the second INDICARE survey

By: Nicole Dufft, Berlecon Research, Berlin, Germany

Abstract: Commercial services for online digital video content are not yet very common in Europe. But new offerings continue to be introduced to the market, and many of them apply DRM systems. In addition, a large share of unlicensed digital video content is available. It will be crucial for successful commercial services that consumers' demands and expectations about what they can do with the content they obtain are met. The latest INDICARE survey provides information about the usage habits of consumers of digital video, their expectations and their willingness to pay for usage rights as well as their awareness of DRM and related issues.

Keywords: survey - INDICARE, broadband, consumer behaviour, consumer expectations, digital video - Europe, France, Germany, Spain, Sweden, UK

Objective of the survey

The goal of the two INDICARE consumer surveys was to gather reliable data on the preferences and behaviour of European consumers with respect to digital goods and on their awareness and acceptance of DRM. The first INDICARE survey was published in May 2005 (Dufft, et. al. 2005) and covered digital music usage and DRM. The current survey's focus is on digital video content: the extent to which European Internet users already use video content from the Internet, the channels through which they obtain it, their willingness to pay for certain usage rights, as well as their knowledge and attitude towards DRM. Included in the survey is the usage of digital video files from various sources. Explicitly excluded are watching videos from physical media such as DVDs or Video CDs on the computer and video games.

The survey was conducted among 2,731 Internet users in five European countries: Spain, Germany, France, the United Kingdom (UK) and Sweden. These countries account for about 64% of GDP and 55% of the total population in the 25 member states of the European Union (Eurostat 2006). Results are representative for all Internet users from age 15 in the respective countries with regard to age, gender, as well as Internet usage frequency.

Digital video usage is not yet very widespread in Europe

Results from the second INDICARE survey show that usage of digital video content is still at a relatively early stage in Europe: even though many Internet users (61%) have made first experiences with watching digital video content from the Internet on their computer, only less than a quarter (22%) do so *frequently*. This compares to 34% of European Internet users that frequently listened to digital music on their computers in 2005.

Downloading video content from the Internet is even less common: 38% have tried to download content, but only 14% do so frequently. However, a quarter of all Internet users show interest in downloading video content from the Internet in the future. This indicates that there is potential for future video download services.

Portable video content does not play an important role to date. However, two results might point towards commercial potential for mobile offerings: first, a comparatively high share of mobile video users *frequently* consumes video content on the go (once tried, they stick with it). Second, almost a quarter of all Internet users – younger users as well as older ones – are interested in using mobile video content in the future.

A lack of knowledge and awareness is the most important reason for not consuming digital video content. A shortage of sufficient bandwidth and high costs are currently not perceived as important barriers, except in Germany.

Significant differences between countries exist

Analysing digital video usage at the country level shows significant differences between the five European countries covered in this survey (Spain, Germany, France, the UK, and Sweden). Spain has the highest proportion of frequent digital video users (46% of all Internet users), followed by France, Sweden, and the UK. Germany has by far the lowest proportion of Internet users frequently consuming digital videos (12%).

These differences can partly be attributed to differences in the Internet population in each country: while Spain has, for example, a relatively low overall share of Internet users in percent of total population, the majority of these users are heavy (i.e. daily) users. Germany, in contrast, has a large Internet population overall, but among these more than half use the Internet only on a weekly basis or less frequently.

Types of video content and channels to obtain it are very diverse

Survey results reveal that the consumption of digital video content is characterized by a high degree of diversity. This diversity relates to the types of video content consumed as well as to the channels accessed to obtain it.

First, we can see that users are trying out many different types of video content and that there is not *the* single "killer content". Music videos are presently the most popular content category, but they are very closely followed by private content (e.g. family and holiday videos), as well as movie previews and advertisements. TV shows and amateur content are currently the least popular content categories. The relatively low importance of amateur content such as video blogs or podcasts contrasts the high attention that this type of content is attracting in the media at present.

Second, there is no single most important channel where users obtain digital video files. Instead, the sources are rather diverse with company websites being the most important source, followed by ripping DVDs and using P2P networks. Service offerings by download portals, mobile operators or TV stations do not yet have a large market penetration.

Diversity needs to be reflected in differentiated usage rights and DRM systems

This diversity in digital video consumption is further aggravated when we look at the different usage rights that consumers are willing to pay for when offered commercial services. A considerable share of users is, for example, willing to pay extra for the right to burn or time-shift full-length movies, while the same is true for a much lower share of users in the case of music videos or TV shows.

The diversity of different content types, distribution channels and expectation of usage rights results in a complexity for content providers and (DRM) technology providers alike, because the diversity needs to be reflected in differentiated service offerings for different content types and channels – particularly with respect to the usage rights granted and the technological measures applied to enforce usage restrictions. As a result, the complexity will affect the way DRM protection is designed, applied and accepted, as the number of technological challenges (e.g. interoperability) is likely to increase.

There is indeed potential for commercial digital video services

Our findings also indicate that there is future potential for commercial digital video content offerings, given that consumers' expectations of what they can do with the content are met. First, a considerable share of consumers indicate that they are interested in watching digital movies and TV shows in the future. Second, many digital video users are interested in services from TV stations, download portals or mobile operators. And third, a significant share of consumers is actually willing to pay for extended usage rights such as burning, time-shifting or sharing.

Digital channels do not necessarily cannibalize existing channels. A considerable share of users are actually watching or downloading digital versions of a specific video via the Internet that they had already consumed through other channels, for example TV.

This indicates that digital video offerings could be well suited as a complement and as a means to exploit the commercial value of movies and TV shows in different stages of their life cycle.

Consumers apparently prefer active over passive content consumption

There are two major advantages that consumers associate with digital video usage: first, being able to watch content wherever and whenever they want (time-shift), and second, being able to avoid commercials. Users are obviously annoyed by the way commercials are placed in traditional media channels today.

At the same time, the high popularity of movie previews and advertisements offered on company websites shows that consumers actively choose to watch smart and entertaining advertisements. This emphasizes, on the one hand, that the Internet can be a very efficient channel for marketers (particularly for the movie industry) to place commercials. On the other hand, consumers increasingly seem to prefer pull (as opposed to push) advertisement.

Consumers’ attitude towards content consumption is apparently about to change from passive to more active consumption behaviour, where viewers are in control of their own schedules and content preferences.

P2P networks play a less prominent role for digital video than for digital music

P2P networks play a less prominent role as a source for digital video than is the case for digital music. 27% of the digital music users, but “only” 14% of the digital video users frequently use P2P networks. However, P2P usage has reached a very significant share in certain countries (e.g. 67% of digital video users in Spain compared to only 11% in Germany).

But we also find that P2P still needs time to be accepted by active P2P users as a legal distribution channel. Even though half of all digital video users appreciate the importance of copyright (i.e. they care if a file is copyrighted or not), only a minority of P2P users would continue to use their network after it was transformed into a licensed offering. Given a significant proportion of users that would be willing to pay extra for extended usage rights, we conclude that the absence of usage restrictions is one of the most important factors besides costs that make P2P networks so popular today.

Consumers are not aware of DRM and usage restrictions

Despite the wide application of DRM technologies that restrict usage rights of digital content today, a large majority of consumers has never heard of DRM and does not know that these technologies are applied. This finding confirms results from the first INDICARE survey among digital music users. In addition, the majority of users that have downloaded digital video content were not informed whether usage rights of the respective videos were restricted or not.

Of those users that know about DRM, almost half were not aware of privacy issues related to DRM, e.g. the fact that DRM technology has the potential to monitor uses of digital content and profile consumption behaviour. One third knows about potential privacy issues but does not mind or simply accepts it.

Bottom line

The results show that digital video content is gaining popularity in Europe. However, many users do not use digital videos on a frequent basis. This has a number of reasons, the most important being a lack of information about offerings and prices. We found that there is no single “killer content” in sight, as was the case, for example, with ringtones for mobile phones. The diversity of the digital video ecosystem (i.e. players, types of content, usage rights, distribution channels) is very likely to add complexity to the respective DRM systems, especially concerning interoperability. Although DRM was more broadly discussed in the recent past, we did not find a rise of awareness for DRM on the side of the consumers.

Sources

- Dufft, Nicole, et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; online available at: http://www.indicare.org
- Dufft, Nicole, et. al. (2006): Digital Video Usage and DRM – Results from a European Consumer Survey, Berlin, February 2006; online available at: http://www.indicare.org
- Eurostat (2006), http://epp.eurostat.cec.eu.int

About the author: Nicole Dufft is a senior analyst at Berlecon Research. She has been analysing a variety of ICT topics ranging from mobile computing and application service providing to DRM. Currently, she works in the field "digital consumer". She is a member of the INDICARE project team. Contact: nd@berlecon.de

Status: first posted 23/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=178

Human factors of DRM – A tour d'horizon
Report about the fifth INDICARE workshop

By: Kristof Kerenyi, SEARCH laboratory, Budapest, Hungary

Abstract: The fifth INDICARE workshop on the "Human Factors of DRM" took place in Budapest on 19 January 2006. The workshop informed about technological, legal and consumer protection aspects of DRM including results from several consumer surveys. Two highlights of the event were the session about content accessibility for the blind, and the presentations from consumer initiatives.

Keywords: conference – INDICARE, accessibility, consumer expectations, consumer interests, consumer surveys, disabled, interoperability

Introduction

The workshop attended by about 40 persons took place in the Informatics building of our university in Budapest on 19 January 2006. It was organised around five thematic blocks: "consumer surveys", "accessibility", "content providers' experience", "consumer rights" and "consumer initiatives". This report does not aim to sum up everything that was said at the event, it is just meant as an appetizer for the full workshop report which will be available for download on the INDICARE web site in March 2006. Below I try to give a very brief coverage of the interesting facts and conclusions for myself.

Consumer surveys

It is very important to explore usage patterns, and other behavioural aspects of users with regard to digital content, since many experts agree that only such business models can win against traditional non-digital distribution channels and illegal offerings which provide more to the consumer, a value added over the common "buy in the store and own a copy" scenario. The common topic of the first block of presentations was what consumers want, how they use content today, in the early age of digital media, and what they know about DRM.

Alapan Arnab, a PhD student from the University of Cape Town started with a strong statement: DRM used to be a jargon for evil technology, also lately when flops like the recent Sony BMG rootkit case did not do any good for the reputation of digital rights management. He analysed some offerings by international companies, and came to the conclusion that terms of purchase were not well advertised, and this increased consumer distrust. He talked about an on-line survey made by his team, which collected 292 full responses to an impressive 91 questions, investigating consumer habits and attitudes towards DRM. Respondents were from countries all over the world. Unfortunately he had to rush through his findings to have time for the introduction of “good DRM”. This, Arnab said, exploits the opportunities in technology for the benefit of the consumer rather than for mega companies, which use DRM only as an enforcement of copyright. DRM could also be used to protect personal data and ensure privacy, which, for example in the case of protecting medical information, would increase consumer trust in technology.

Dr. *Péter Benjamin Tóth* from ARTISJUS, the Hungarian Bureau for the Protection of Authors’ Rights, introduced the results of two surveys to support his statement that Digital Rights Management may not be the best solution to address today’s problems, instead Collective Rights Management – which term he preferred instead of calling ARTISJUS a collecting society – could be a better choice. He argued by drawing up the formulas based on which levies are collected, and supported his point with the figures derived from the two surveys. Examining content copied to blank CDs and DVDs, both in a representative survey done by GfK (Gesellschaft für Konsumforschung), and in another done by Free Association at the Sziget festival (the biggest music festival in Central-Europe, therefore the respondents here were “power users” of music) he concluded that at least 90 percent of data burned to blank media was content protected by copyright, but subject to free copying. From this he derived the calculated amount of levy per carrier that *should be* a fair compensation for authors, and then showed the *actual amount from use*. Interestingly, even though the amount from use was at least 5 times smaller than the smallest calculated amount, most consumers think even this small amount unfair for themselves. Levies have to be held so low, Tóth said, because there is a strong black market presence also on the market of blank CDs and DVDs, with which they have to compete, and consumers, here too, vote with their wallets.

Philipp Bohn, analyst and INDICARE team member from Berlecon Research, talked about the results of the first consumer survey on digital music (Dufft et. al. 2005) and introduced the second consumer survey on digital video use, which was at that time being prepared, although it is now online on the INDICARE web site (Dufft et al. 2006).

Accessibility

Norbert Márkus from the KFKI Laboratory of Speech Technology for Rehabilitation, and also a jazz pianist and composer gave a very extensive introduction to the history of accessibility on the computer. He said that in the 80s and early 90s blind people were in a not much worse situation than their sighted colleagues. Then with the coming of window-based systems (also Microsoft Windows) their situation got much worse, but by today the technology has improved to work again with the latest computers. However, nowadays the problems are due to carelessly designed layout. DRM means another difficulty for accessibility, since, though allowed by copyright law, making content accessible for the blind would mean in many cases making it available for content pirates, too. At least the content publishers have this opinion, which, again, means great difficulty for blind or partially sighted people. Márkus talked also about musical scores in Braille form, which are represented in computers as BMX (Braille Music XML). The situation with this is the same as with other content: publishers fear of pirates.

Hugh Huddy from the Royal National Institute of the Blind, head of Campaign for good E-Document Design, gave a talk about new opportunities and hurdles that e-documents pose for the blind. After demonstrating some special programs that make laptops, mobile phones and other electronic staff blind-friendly, Huddy talked about a new world where paper is gone. This opens up the opportunity for blind and partially sighted people to have an equal chance in life for accessing information, but he said, just as we create artificial barriers for handicapped people in the physical world, we are re-creating such barriers for the blind in the electronic world. He emphasised the responsibility of technology companies, policy makers and also users to create a world where the “Right to Read” is reality.

Content providers' experience

The rather short session where two large telecommunication providers, T-Online and T-Mobile, introduced their view of DRM inspired a lively debate.

Miklós Gyertyánfy from T-Online talked about the T-Group member's music offerings and use of DRM (also covered in Kerenyi 2005), and also introduced their video-on-demand service. They chose Microsoft's solution because it is compatible with most players. He also underlined that while they have the intention, it is not yet possible to introduce electronic video sell-through (download and burn), since MS technology does not support it. Gyertyánfy talked about T-Online's new pilot project with IPTV, into which they will incorporate all previous DRM-related experience. The most important, he said, was: users don't want to understand technology, just use the content anytime, anywhere.

Péter Verhás from T-Mobile talked about the technical solutions which are used to protect content. He talked about OMA DRM 1, which is used by the vast majority of phones today, using the phone as authentication token, not the SIM card, which means that interoperability was not even an issue when the system was designed. However, as in the case of T-Online, they provide a "reload" service for the new device: the content provider has a record of what the consumer has purchased, and enables her to re-download the content for the new device. Registering what a consumer has purchased also gives the advantage for the content providers of knowing the customer, and his habits. This and the contractual relationship between the telecommunications provider and the consumer puts mobile operators at an advantage. Verhás had another very important point in his presentation: he emphasised that while mobile phones are becoming the DRM enabler devices today, their usage pattern differs between countries, thus cell phones do not enable content usage and DRM in the same way across cultures.

Both speakers attracted a huge wave of complaints and questions regarding their services and attitudes towards consumers: it seemed like as they were the only representatives of the content providers, some workshop participants blamed them for the current, in many cases unfriendly situation with real world content offerings.

Consumer rights

One of the questions most interesting to consumers is their rights, and legal state when dealing with digital content. Consumers are often criminalized, advertisements on the streets and television spots emphasise that downloading music is illegal. On the other hand, content providers often impose conditions that are unfair and in many cases unacceptable for consumers.

Lars Grøndal from BEUC on secondment from the Consumer Council of Norway, talked about standard terms of contracts regulating how consumers can use digital products legally, and DRM controlling how consumers can use digital content de facto, and the two not meeting in many cases. With a case study on iTunes' standard terms he illustrated how unfair terms and conditions of purchase can be. Grøndal mentioned that consumers are not in a very bad situation, since for example in Norway, one can legally circumvent DRM measures either to achieve accessibility or to be able to play purchased content on another player. He concluded his speech with the statement that "business interests are not the only that deserve protection" (cf. also Grøndal 2006).

Dr. *Anikó Gyenge* from the Hungarian Ministry of Justice talked about the well-known controversy between copyright law and TPM (technical protection measures). She emphasised that not all of the technical functions can be legally interpreted, therefore not all measures are protected by copyright law. She talked about free use and to what extent DRM restricted legal copyright exemptions. In the end she concluded, that while consumers might be in a not too favourable situation, there is a difference between written law and enforced law: since the regulatory system is hard to interpret in practice, judges in many cases do not apply the code – to the benefit of consumers.

Matthias Spielkamp, editor of iRights.info introduced their project to the workshop participants. He said that they examined the contract terms of three music services available in Germany: iTunes, Musicload and Sony Connect had 33, 18 and 55 pages of usage terms respectively after he copied and pasted them into Word, and corrected their font size and layout. iRights.info, a project funded by the German Ministry of Consumer Protection, provides additional information, since, as Spielkamp pointed out, from these terms and conditions "no one is able to understand what is going on". Fairness, openness, reliability, independence and finding the correct balance between alternatives are their main approach. On their web page consumers can find more than 40 texts on basic aspects of law and usage, and there are news every week. iRights.info follows an interdisciplinary approach and uses current media tools to educate German consumers about their rights regarding digital content and DRM.

Consumer initiatives

Martin Springer, a private contributor to the Digital Media Project, started his presentation with a case study: Every couple of years the soccer leagues make their exclusive license deals with three or four content providers, and thus they force their fans to either accept their new proprietary DRM standard, or stop watching the games. Thus if a football fan in Germany wants to follow his team's matches in national and international games, he needs to subscribe to several service providers and network providers, and spend a lot of money for buying incompatible receivers and to subscribe to unnecessary programme packages. He concluded that the industry uses DRM as a weapon against competitors, trying to lock consumers into a particular DRM scheme and particular business models. Innovative media usages like sharing content among soccer fans from different European countries are impossible. Springer suggested that consumers should get involved in DRM standardization with the goal of creating a standard DRM that is open and acceptable for both consumers and rights holders. He introduced the DMP project (Jeges 2005; Jeges and Kerenyi 2005), in which he works because he intends to defend concepts like privacy and End-user Rights in a DRM standard.

Balázs Bodó, assistant lecturer and researcher from the BUTE Centre for Media Research and Education, introduced the Silent Library Project, a commons-based peer production. First he illustrated with figures, that both on the Hungarian, and US markets, considering both books and feature films, around 20 per cent of the titles that have been published within the last 15 years are still available for purchase. The simple reason is lack of shelf space, he said. However, there is still a considerable market demand for those titles not on the shelves. Each is under copyright, but they are not available from legal sources. The Silent Library Project is an illegal movement, a group of people who started scanning and digitizing such titles, and sharing them with each other, making them available again. DRM has a completely different approach, he said: by centralization and access hierarchy they tend to re-create scarcity in the digital world, similarly to the physical world. Bodó illustrated the world in 2050 with an imagined scenario, where all works from 2010 will probably be available secured by unbreakable DRM. In this world, when no marketing is behind a product (it is not in the 20 percent), and commons-based networks (like SLP) are shut down, our knowledge, our common experience will shrink. Culture is a common good – he finished his talk.

Bottom line

Zoltán Hornák, INDICARE project member from SEARCH concluded the day. Since the workshop moved along different stream, each related to consumer aspects, the conclusions he drew from the whole day's presentations and programme were rather diverse.

From the surveys we can learn that there is a clear demand from consumers to obtain content, even paid content, however, if consumers consider the offerings unfair, they will not go with them, and choose alternative channels. Furthermore, consumer expectations of traditional usages must be supported to create viable DRM systems.

In the accessibility session we could learn about the difficulties that blind or other disabled people may face when accessing even unprotected content, and also the controversies of DRM and accessibility. And although nowadays accessibility of content and DRM can work together, we must take care that in the digital world, a world that we can design from the basics, we do not recreate the barriers that are present for some people in the physical world.

The content providers emphasised that DRM helps them to know their consumer and create new business models, while consumer rights experts doubted this statement. From the rights session we learned that consumers are not in a very bad position after all, because in some countries doing “things in the grey”, like downloading or freeing DRM-protected content is not illegal according to law, and even if it is forbidden, if judges do not enforce it, code does not have much effect. In any case, informing consumers about rights in a clear and understandable manner is a very important issue.

At the end of the workshop we could hear about two consumer initiatives, one of which tried to work out a better, interoperable and thus for the consumers more acceptable, DRM system, and the other completely rejected DRM and tried to create an (under)world without DRM.

My personal conclusion from the workshop was: consumers, and their wishes must not be neglected any more!

Sources

- ► Dufft, Nicole, et. al. (2005): Digital music and DRM – Results from an European consumer survey. http://www.indicare.org/tiki-download_file.php?fileId=110
- ► Dufft, Nicole et. al. (2006): Digital video usage and DRM – Results from a European consumer survey. http://www.indicare.org/tiki-download_file.php?fileId=170
- ► Grøndal, Lars (2006): DRM and contract terms. INDICARE Monitor, Vol. 2, Number 12, February 2006; http://www.indicare.org/tiki-read_article.php?articleId=177
- ► Jeges, Ernő (2005): Digital Media Project – Part I. Towards an interoperable DRM platform. INDICARE Monitor, Vol. 2, No 4, June 2005 ; http://www.indicare.org/tiki-read_article.php?articleId=116
- ► Jeges, Ernő; Kerényi, Kristóf (2005): Digital Media Project – Part II: Chances of an open standard. INDICARE Monitor, Vol. 2, No 6, August 2005; http://www.indicare.org/tiki-read_article.php?articleId=134
- ► Kerényi, Kristóf (2005): Online music in Hungary. INDICARE Monitor, Vol. 2, No 7, September 2005; http://www.indicare.org/tiki-read_article.php?articleId=138

About the author: Kristóf Kerényi is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=182

DRM and contract terms

By: Lars Grøndal, BEUC, Brussels, Belgium

Abstract: In every day life consumers are frequently accepting standardised contractual and technological terms that they have little or no understanding of. Some of these terms are generally unfair and do not stand up to legal scrutiny. In this article iTunes Music Store's Terms of Service is used as an example of a standard contract containing unfair terms.

Keywords: legal analysis, case study - consumer expectations, consumer protection, online music, standard contracts, unfair terms

Introduction

Standard contracts are written terms that regulate how consumers legally can use purchased products. DRMs on the other hand are technical measures that control how consumers *de facto* can make use of digital goods and services. Amongst other things, DRMs frequently enforce standard contract terms.

Both DRMs and standard terms are seldom open to individual negotiation – either the consumer accepts them or the consumer will have to take its business elsewhere. If consumers had a wide variety of easily comparable terms this would not be a problem. But as the situation is today, with opaque and often standardised conditions, consumers are facing insurmountable difficulties in obtaining fair terms. Even the legally trained consumer will have trouble getting a proper understanding of all the terms you meet in every day life.

Just like other business practises, standard terms and DRMs do not always stand up to legal scrutiny. In this article I will focus on DRM and contract terms consumers meet when purchasing music online. More specifically, I will look at some of the terms in iTunes Music Store (iTMS, iTunes) Terms of Service (ToS).

At the outset I would like to emphasise that these terms are not unique to iTunes. There are many other digital products where similar conditions apply: software, videogames, CDs, DVDs, etc.

A number of provisions in the iTMS Terms of Service are questionable both in relation to community and national law. I will focus on three terms which are of particular interest in relation to DRM:

- iTMS ability to unilaterally change terms and conditions,
- The limitations on liability, and
- The limitations on interoperability.

Unilaterally change terms and conditions

According to iTunes Music Store Terms of Service, Apple reserves the right, at its sole discretion, to change the way customers can use downloaded material (iTMS 2006).

It says in article 20 that:

> "iTunes reserves the right, at any time and from time to time, to update, revise, supplement, and otherwise modify this Agreement and to impose new or additional rules, policies, terms, or conditions on your use of the Service."

Furthermore, in article 9d it says that:

> "[Y]ou acknowledge that you may no longer be able to use Products to the same extent as prior to such change or discontinuation [...]."

This entails that Apple reserves the right to unilaterally change the way a file can be used after the purchase. For instance, Apple could limit the number of times an iTMS file can be burned onto a CD. If you buy a music file on iTMS today you can burn a playlist 7 times. According to the ToS, Apple is entitled to limit the number of playlist you can burn from the same file tomorrow.

Amendments in the terms and conditions can be enforced by changing the DRM.

A study by Intertek (2005) found that although it would be technically challenging, it is possible to change the DRM on already downloaded material. Boing Boing, a tech news site, reported last year that iTunes Music Store has changed customers' usage rights to material customers already had on their computer (Boing Boing 2005). By installing updates to the iTMS software, customers lost the ability to:

- stream unlimited over the local network (down to 5 times per 24 hours),
- stream over the internet,
- burn a playlist 10 times (down to 7).

Changes might not be enforced by changing the DRM, but simply by amending the Terms of Use. According to the legal terms:

> "It is your responsibility to check these Terms of Use periodically for changes."

If a costumer uses the file in a way which was allowed at the time of purchase, but is no longer permitted, the consumer is in breach of contract. The Terms of Service sets out a range of sanctions which iTMS can apply as they see fit.

Article 14a of the terms state that:

> "If you fail, or iTunes suspects that you have failed, to comply with any of the provisions of this Agreement, […] iTunes, *at its sole discretion, without notice to you may* [my italics]: (i) terminate this Agreement and/or your Account […]; and/or (ii) terminate the license to the software; and/or (iii) preclude access to the Service (or any part thereof)."

This entails that the customer could be banned from iTMS at Apples sole discretion and without notice just because she failed to keep herself regularly updated on the Terms of Use.

The right to unilaterally change terms of contract is considered an unfair term according to Directive 93/13/EC (EU 1993) on unfair terms in consumer contracts. Consumers do not expect new terms and conditions being applied retroactively; if you buy a product today and you can use it in certain ways, you expect that you will be able to use the product in the same way tomorrow.

In the annex to the Unfair Terms Directive there is a non-exhaustive list of terms which may be regarded as unfair. Letter j is of particular interest here:

> "enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract;"

Limitations on liability

Recent examples have shown that DRM systems can cause severe security risks. The copy-protection technology that has been used on some Sony BMG CDs, XCP, left consumers' computers open to attacks (for more information on XCP see EFF 2006).

According to another tech news site, The Register, serious security flaws have recently been discovered in iTMS (Leyden 2006). iTunes Music Store, through its conditions, disclaims all liability for attacks on consumers' computers, even if it is caused by security flaws in Apples DRM, Fairplay.

Article 18a (ii) of the Terms of Service says that:

> "iTUNES DOES NOT REPRESENT OR GUARANTEE THAT THE SERVICE WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND iTUNES DISCLAIMS ANY LIABILITY RELATING THERETO." [The paragraph is for some reason all in capital letters in the iTMS Terms of Service].

This type of term is not specifically mentioned in the annex to the Unfair Terms Directive, but the list is not exhaustive. Consumer protection legislation in many Member States (the Nordic countries for instance) prohibit limitations on consumers' statutory right to damages.

Pursuant to the Norwegian Consumer Contract Act (2001) section 33, vendors are liable for damages caused by the purchased product. Contractual limitations on consumers' right to damages are void. This law is not directly applicable when downloading music, but it is indicative of the fairness of the term. Consequently, this term should be considered unfair under the Unfair terms Directive.

Interoperability

Fairplay, the DRM used by iTMS, prevents the consumer from using other players than Apple's iPod to play music purchased from iTunes.

The contract also limits which players can be used. Article 9 b states that:

> "You shall be authorized to use the Products on up to five *iTunes-authorised devices* [my italics] at any time. […] You shall be able to store Products from up to five different Accounts on *certain devices, such as an iPod* [my italics], at a time."

The only portable player authorised by Fairplay is iPod. Thus, the contract only allows consumers to use iPod to play files downloaded from iTunes.

Consumers can easily get around this limitation. As the test (Intertek 2005) commissioned by BEUC shows, Fairplay can be erased and the file converted to MP3 format by burning a CD with iTunes files and then subsequently ripping them back to the computer.

If a consumer uses this method to make use of a different player, e.g. a Creative player, this would not be in accordance with the contract.

Tying the consumer to use a certain player, however, can be contrary to community and national legislation. Consumer law, competition law and even copyright law can be used to combat this type of business practise.

It has been discussed whether iTune's refusal to licence Fairplay to competitors could constitute an abuse of dominance contrary to article 82 of the EC Treaty. This is doubtful however; both because of the difficulty in establishing dominance and because of the European Court of Justice' reluctance to impose mandatory licensing (see Reckon 2006).

Consumer protection rules could be an easier option. One could argue that contractual obligations tying iTunes customers to one specific portable player is unfair pursuant to the Unfair Terms Directive.

A French consumer group, UFC Que Choisir, has initiated legal proceedings against Apple, claiming that tying iTunes customers to use iPod and vice versa, is not in accordance with the French consumer code article 122 which says that:

> "It is prohibited to refuse to sell a product, or supply a service, to a consumer without a legitimate reason, and to make the sale of a product subject to the purchase of a minimum quantity, or to the accompanying purchase of another product, or another service, as well as making the provision of a service subject to provision of another service, or to the purchase of a product."

Depending on national legislation, copyright law itself can be used to combat the lack of interoperability. Take for instance the Norwegian Copyright Act that implements Directive 2001/29/EC (the Copyright Directive). Circumventing effective technological measures is prohibited under section 53a of the Copyright Act. In the third paragraph there is an exception to the anti circumvention provision: effective technological measures can be circumvented to play legally acquired works on relevant players. According to some commentators this provision gives consumers the right to circumvent Fairplay in order to use other portable players than iPods (Vigmostad 2005). The Norwegian Consumer Ombudsman has consistently held that standard contractual terms limiting consumers' statutory rights are unfair and void under the Norwegian Marketing Control Act (1972) section 9a .

A different question is whether Fairplay is protected under the Norwegian Copyright Act or the Copyright Directive at all. Both section 53a and article 6 of the Copyright Directive only protects *effective* technological measures. In the preparatory works to the Copyright Act, copy-protection on CDs that could be erased by simply writing with a pen on it was characterised as an ineffective protection measures. The copy-protection technology on files downloaded from iTunes is erased simply by burning a playlist. This is very easy to do and is permitted under the contract.

Having said that, making it easy to get around DRMs, and especially those that curtail competition, is a definitively a good thing for consumers and I would not like to see a more effective DRM being implemented in the future.

How do we deal with these kinds of terms?

The Unfair Terms Directive article 7 obliges Member States and other parties to the EEA (European Economic Area) agreement to have "adequate and effective means […] to prevent the continued use of unfair terms".

In the next paragraph of the article it says:

> "The means referred to in paragraph 1 shall include provisions whereby persons or organizations […] may take action according to the national law concerned before the courts or before competent administrative bodies […] to prevent the continued use of such terms".

In Norway the Consumer Ombudsman deals with unfair contract terms. According to the Marketing Control Act Section 9a:

> "Terms and conditions which are applied or are intended to be applied in the conduct of business with consumers can be prohibited if the terms and conditions are considered unfair".

Terms and conditions can mean both traditional written terms, but also technical ones like DRMs.

The Consumer Council of Norway has complained to the Consumer Ombudsman in order to get iTunes terms amended. The Consumer Council has also argued that certain aspects of the DRM Fairplay are unfair and should be amended (Consumer Council of Norway 2006; see also Singstad 2006)

Bottom line

To conclude, there are ways of combating the unfair use of DRMs with today's legislation. However, the current legal regime does not fully take into account the unique characteristics of digital products. European and national consumer legislation focuses mainly on traditional tangible products bought in traditional ways.

Also, the Community legislation being proposed and adopted in this area predominately caters to business interests and does not take into consideration the dire consequences for consumers. Take for instance the Commission's proposal on harmonisation of criminal measures on IPR infringements (EU 2005). According to article 3 of the proposal, intentional infringements of IPRs on a "commercial scale" must be treated as criminal offences. One of the justifications of the proposal was that the "[i]ncreasing use of the Internet enables pirated products to be distributed instantly around the globe". The Directive does not require a profit motive to apply. Thus, it seems that illegal file-sharing through P2P networks are covered by the Directive. Consequently, the proposal can potentially criminalise the technologically proficient youth of Europe. The Commission withdrew the original proposal for competency reasons. To our knowledge the Directive will be reissued in March without substantial amendments. For other examples of EU IPR initiatives where consumer considerations are absent, see Kutterer 2005.

As a response to the lack of public interest considerations in EU policy on IPR, BEUC launched a campaign for consumers' digital rights in November 2005 (BEUC 2005). We believe that business interests are not the only ones which deserve protection in the digital environment. Our aim with the campaign is to raise awareness in this field both among policymakers and consumers and to promote a better legal framework for consumers.

Sources

- BEUC (2005): consumers digital rights: http://www.consumersdigitalrights.org/cms/index_en.php
- Boing Boing (March 16, 2005): Apple steals iTunes customers' paid-for rights to stream http://www.boingboing.net/2005/03/16/apple_steals_itunes_.html
- Consumer Council of Norway (2006): Complaint against iTunes Music Store; http://forbrukerportalen.no/filer/Complaint%20against%20iTunes%20Music%20Store.pdf
- Electronic Frontier Foundation (EFF) (2006): Sony BMG Litigation Info; http://www.eff.org/IP/DRM/Sony-BMG/
- EU (1993): Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Official Journal L 095, 21.4.1993, pp. 29-34; http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31993L0013&model=guichett
- EU (2005): Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights 2005/0127(COD), http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0276en01.pdf
- European Court of Justice (2004): Judgment of the Court (Fifth Chamber) of 29 April 2004, IMS Health GmbH & Co. OHG v NDC, C-418/01
- French consumer code: Article L122-1: http://195.83.177.9/code/liste.phtml?lang=uk&c=61&r=2133
- Intertek Research & Performance Testing (2005): Online Music Download Services. Technical Report 63028 Issue 2, September 2005; http://www.consumersdigitalrights.org/mdoc/OnlineMusicDownloadServices_TechnicalReport_90041.pdfi
- iTunes Music Store (iTMS) (2006): Terms of Service and legal terms http://www.apple.com/uk/support/itunes/legal/terms.html and http://www.apple.com/legal/terms/site.html
- Kutterer (2005): Some of the reasons for BEUC's Campaign on Consumers' Digital Rights. INDICARE Monitor, Vol. 2, Number 10, December 2005; http://www.indicare.org/tiki-read_article.php?articleId=162
- Leyden, John (2006): Apple bitten by iTunes security bugs. The Register Wednesday 11th January 2006; http://www.theregister.com/2006/01/11/itunes_vulns/
- Norwegian Consumer Contract Act (2001): http://www.lovdata.no/all/nl-20020621-034.html
- Reckon LLP (ed.) (2006): iTunes, DRM and competition law. Reckon Open; http://www.reckon.co.uk/open/iTunes
- Singstad, Jo (2006): iTunes' questionable terms and conditions; http://forbrukerportalen.no/Artikler/2006/1138119849.71
- Vigmostad, Tobias (2005): Digital Rights Management Systems as they apply to the Norwegian Intellectual Property Act, Section 53a, Paragraphs 1 and 3, 2nd Sentence; http://www.dagbladet.no/download/oppgave.doc and http://www.dagbladet.no/kultur/2006/02/01/456502.html
- The Norwegian Marketing Control Act (1972): http://www.forbrukerombudet.no/index.gan?id=706&subid=0

About the author: Lars Grøndal is a legal advisor currently working for BEUC, the European Consumers' Organisation. He is on a secondment from the Norwegian member, The Consumer Council of Norway. Contact: lars.grondal@beuc.org or lars.grondal@forbrukerradet.no

Status: first posted 23/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=177

Copyright law as an enigma for laypersons and the need for iRights.info

By: Matthias Spielkamp, iRights.info, Berlin, Gemany

Abstract: Implementation of the European Union Copyright Directive's provisions into member states' laws has led to increased confusion about copyright issues for consumers. This is particularly relevant at a time when more and more uses of digital media are regulated by copyright. Rights holders, especially large, multi-national companies, are not willing to inform consumers unbiased. Hence the continued need for publicly funded, impartial consumer information, preferably on a multi-national, multi-language EU level.

Keywords: case study – file sharing, copyright law, EUCD, consumer information, piracy

Why confusion about copyright law is a consumer issue

Five years ago, the European Union's Copyright Directive (EUCD) finally, after four years of negotiations, passed the EU's legislative process. Since then, almost all EU member states have devised and adopted laws to – more or less – implement the directive's provisions into their respective authors rights or copyright codes (with the exception of France, Spain and the Czech Republic). Following its approval by the Council of Ministers, the chairman of the European Commission's Legal Advisory Board Taskforce on Intellectual Property – among many others – criticised the EUCD for its ambiguity: "It does not increase 'legal certainty', a goal repeatedly stated in the Directive's Recitals (…), but instead creates new uncertainties by using vague and in places almost unintelligible language"(Hugenholtz 2000). In the case of Germany, these new uncertainties have carried over into the country's revised authors rights code, which came into effect in September 2003. To give an illustration of what this entails for regular users of digital media and the Internet, I will first provide a case study of the legal implications of file sharing in Germany. I will then briefly explain the role of the iRights.info (cf. sources) as a consumer information portal on copyright issues.

Case study: File-sharing and the law in Germany

Many uses of file-sharing networks are completely legal. Some people know this, some may take it for granted, but to some people this will sound rather surprising. Reading newspaper articles on the topic or watching TV reports, one can certainly get the impression that everything that has to do with file-sharing is so called "illegal piracy". But this is not the case.

Sharing someone's own works – texts, music, pictures, videos, software, games, animations and so on – is completely legal. Or, to be more specific: It is legal to share works if the person sharing them holds the rights to these works. For example, more and more companies put files on the web to share as well: music for promotional purposes, movie trailers and the like.

In addition to works someone owns, sharing is allowed for works the copyright holder allows to be shared – this sounds obvious, but one has to be aware that the rights holder must specifically assign those rights. This is done quite often, though, i.e. with works under Creative Commons licences (cf. sources), the GPL (GNU General Public Licence) (cf. sources) and many others.

Then there are works in the public domain. An example for this is the Project Gutenberg (cf. sources), where scholars, students, and activists digitize classical texts from Aristotle to Zola and make them available in a searchable database.

In a majority of cases, file sharing networks are used to break the law

Most uses that are actually practiced on today's file sharing networks are illegal, though. The vast majority of music, films, software, and texts are copyrighted and the rights holders prohibit sharing. Since the so called “first basket” (first round) of the German copyright revision came into force in September 2003 (Bundesministerium 2003), it is illegal for individuals to make available works in a file-sharing network without holding the rights to them – which is the majority of works on file-sharing networks today. So most of the actual uploading being done is clearly illegal under German law.

Downloading still considered legal in Germany by many

Downloading is a different matter, though. If a user in Germany downloads a song from a file-sharing network, it is seen as a duplication – a copy of the song. If this copy is for private use, it is perfectly legal – like copying a CD or a videotape. This permission is granted by an exception to copyright (“Schrankenregelung”), resembling – not equalling – the fair use provision in US copyright law. Of course it is not allowed to sell or lend this copy, because then it would be a commercial use, which is prohibited.

But copying for private use is only allowed if the original is lawful; if the work from which the copy is made is itself “evidently an unlawful copy”, it is prohibited. But how can someone tell whether it is evident that this work found on the file-sharing network was produced unlawfully?

This question is very hard to answer. Imagine you find a copy of the movie “Independence Day” on the file sharing network Kazaa and decide to download it. Is this lawful?

It might well be. It has been shown on TV in Germany. So someone might have recorded the TV broadcast on his PC and converted the recording into a digital file. With this he is making a copy for private use, which is perfectly lawful. If he put the file on a file-sharing network, though, he would clearly be breaking the law because he doesn’t have the right to distribute the movie, or to make it available. But someone downloading the file would not be breaking the law, because it was not evident that the copy that was made available was produced illegally. It was illegal to make it available, but the subsequent copying of the file is legal.

The difference between “Independence Day” and “Walk the Line”: obvious or not?

Confusing? Certainly, but it gets even worse. Imagine someone finds a copy of “Walk the Line” on a file-sharing network. Is it legal to download it? As we have seen, it would be, if it were not obvious that the copy found on the network was produced illegally. But is it obvious that it is a copy produced illegally? To answer this question, one has to be able to answer the following questions: Has the movie in question been broadcast on TV? Answer: Probably not, it just came out in Germany, it is a big production and in cinemas at that moment. Has it been released for home viewing?

Answer: This is difficult to determine. It is a rather new movie. But then, US movies are often releeased in the US long before they come to theatres in Europe (i.e., the drama “House of Sand and Fog”, which was released in the US on December 26, 2003, came to theatres in Germany on February 17, 2005 – more than a year later. At the time the movie was still showing in German theatres the DVD was already available in the US, where it was released March 30, 2005 (cf. House of Sand and Fog). And if the person planning to download the movie lives in a small city with only one cinema, then she is familiar with the situation that movies come out a lot later there than in Berlin, Madrid, or London. So if it came out in the US a year ago already, it might have been released for home viewing in the US a while ago. Therefore someone could have bought the DVD of the movie, made a private copy of it and put it on the file-sharing network – this way it would be legal to download it.

But what if the DVD is copy-protected? Because of anti-circumvention legislation, it may be illegal to make a copy, even for private use. For one, all these laws are very complicated to understand and interpret, even for legal professionals. Additionally, how would a downloader know whether “Walk the Line” is copy-protected or not? In our sample case, he does not even know whether it has been released on DVD yet.

So after exhaustive and careful deliberation the user decides to download the movie. By doing this, he brakes the law – at least that is what the rights holders say. Because “Walk the Line” has not been released for home viewing to date, the file on the file-sharing network has to be a copy someone made with his video camera in a cinema, and therefore illegal. So the user has not only waited for hours for an abysmally bad and grainy copy of “Walk the Line” to download onto his PC, he also has the studios demanding damages.

iRights.info: A continuing effort needed to inform citizens about copyright issues

The example analysed above shows the complexity of the law and, as a result, the difficulty in understanding and interpreting it. This case can only illustrate the situation in Germany, because EU member states’ jurisdictions differ widely in the concept of copyright and authors rights codes in general and the implementation of the EUCD in particular. Judging on the basis of media reports from different countries, it can be safely assumed that in many cases their situation is comparable to that in Germany.

To expect rights holders to provide balanced information on copyright issues is futile. Various analyses of their campaigns targeted towards consumers (e.g. Spielkamp 2005; Djordjevic et al. 2005) have shown that their only identifiable interest lies in causing fear, uncertainty and doubt in regard to what rights consumers have using digital media, in order to convey the impression that all uses are subject to permission by rights holders.

Impartial information on copyright issues sought by consumers

In Germany, one approach to mitigate consumers’ information deficit is iRights.info , a web site mainly funded by the Ministry for Consumer Protection. INDICARE Monitor readers might already know about iRights by the interview with its legal expert *Till Kreutzer* (Kreutzer 2005). Four part time editors, all specialised on copyright issues in their respective professions (law, art, information science, journalism) compile a wide range of articles illuminating the implications of every day uses of copyrighted works: under what circumstances it is legal to copy CDs, post pictures in your weblog, use samples in your own music, and so on.

The web site currently receives more than 1.500 unique visits per day, showing a high demand for this kind of information. This impression is substantiated by the fact that frequently, people send e-mails to the editors, asking specific questions they do not find answered for in the articles. In these cases, because of legal regulations in Germany, the editors cannot provide legal advice regarding specific cases, but attempt to point to articles and information that should help answer the case in question.

The nature of users’ inquiries so far clearly back the stated assumption about the nature of copyright regulation. Most of them show a helplessness regarding the interpretation of the law when it comes to uses of digital media both in situations where people would like to use digital content and when they would like to create new works.

iRights.info as a pan-European project

Funding for iRights.info will run out at the end of March, 2006. As argued above, the notable deficit of this kind of relevant and impartial information about copyright and authors rights issues for consumers remains. iRights.info will therefore attempt to widen the scope of iRight.info to make it a pan-European project and secure funding from the European Union. In case of an interest in cooperating towards this aim, please contact the author at ms@iRights.info.

Sources

- Bundesministerium der Justiz: “Neues Urheberrecht ab morgen in Kraft”, http://www.kopien-brauchen-originale.de/enid/5j.html, text of law available at http://217.160.60.235/BGBL/bgbl1f/bgbl103s1774.pdf (accessed February 15, 2006)
- Creative Commons Website, http://creativecommons.org (accessed September 2, 2005)
- Djordjevic, V; Kreutzer, T.; Spielkamp, M.: iRights.info. Informationsgesellschaft und Urheberrecht. Log In 136/37 (2005), pp.118-122
- Free Software Foundation: GNU General Public License, http://www.gnu.org/copyleft/gpl.html. (accessed February 15, 2006)

- Hugenholtz, B.: Why the Copyright Directive is unimportant, and possibly invalid. European intellectual property review (EIPR) 11, 2000; http://www.ivir.nl/publications/hugenholtz/opinion-EIPR.html (accessed February 15, 2006)
- House of Sand and Fog-website: http://www.dreamworks.com/dvd_features_hosaf.html (accessed February 15, 2006)
- iRights.info: http://iRights.info
- Kreutzer, T.: Copyright - complexity - confusion. The basic approach to copyright needs rethinking. INDICARE-Interview by Nicole Dufft. INDICARE Monitor Vol. 2, No 4, 24 June 2005; http://www.indicare.org/tiki-read_article.php?articleId=119
- Project Gutenberg: http://www.gutenberg.org (accessed February 15, 2006)
- Spielkamp, M.: iRights.info. The need for reliable and trustworthy consumer information after copyright revision in Germany. Axmedis 2005, Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution: Volume for Workshops, Industrial and Applications Sessions, p. 113-118

About the author: Matthias Spielkamp is an editor at iRights.info. He publishes in national newspapers, magazines, online publications (Die Zeit, FAZ, SZ, taz, Spiegel ONLINE, Golem.de, telepolis etc.) and his weblog immateriblog.de. He can be contacted at ms@iRights.info.

Status: first posted 23/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=176

Christophe R. vs Warner Music: French court bans private-copying hostile DRM

By: Natali Helberger, IViR, University of Amsterdam, The Netherlands

Abstract: France is one of the European countries where a particularly vivid public discussion about DRM and the private copying exception took place. This is thanks to the efforts of French consumer organisations that initiated a number of court cases dealing with complaints of consumers about CDs and DVDs that could, among others, not be copied and ripped because of technical protection measures in place. This article discusses the latest DRM decision in France, a decision that went one step further than its predecessors when dealing with the difficult question of the relationship between DRM and private copying.

Keywords: legal analysis – consumer expectations, copyright exceptions, copyright law, court decision, DRMS, EUCD - France

France developed important body of case law

That there is a conflict between DRM use and consumer interests has been demonstrated over the past three years by the number of cases about CDs and DVDs that could not be played on car radios, PCs and laptops or could not be copied and ripped because of installed technical protection measures. Over the course of three years, French courts have developed the argument that the ability to play a CD or a DVD on different devices, including the radios from different brands of cars or different kinds of computers, constitutes an essential characteristic of a CD or DVD.

Consequently, where phonogram or DVD producers failed to warn consumer about possible incompatibilities between content and consumer hardware, the former could be held liable because of misleading behaviour towards the consumer (Tribunal de Nanterre 2003a, Tribunal de Nanterre 2003b). More complicated, and less promising for consumers, was the situation regarding DRM and private copying. Unforgotten is the finding of The Tribunal Paris in one of the earlier DRM cases in France, that there was no "right to private copying" (Tribunal Paris 2004 – the "Mulholland Drive" case). This was a black day for the private copying exception. Worse, it delivered the content industry a standard argument which is still regularly evoked by CD and DVD producers when defending their policy of letting the private copying exception die a forceful, electronic death. However, the last word in this matter was not yet spoken, and a year later the Court of Appeals concluded that there may be no right to private copying, still the private copying exception formed a restriction to the exclusive exploitation rights conferred to right holders, and as such was not at the disposition of DRM users (Court of Appeals, Paris 2005).

There was a new decision on 10. January 2006 about DRM and private copying, on which we will report here. The timing of the case, one might want to add, could not have been better: presently pending before the Assemble Nationale, the French Parliament, is the long-overdue proposal for a revised copyright law that implements the provisions of the European Copyright Directive from 2001, including the section on the swelling conflict between technological protection measures and copyright law. The present article will have a closer look at how the Tribunal de Grande Instance de Paris approached the matter. In a subsequent article (Helberger 2006), we will have a closer look at the pending reform of French law and the implementation of the provisions in the European Copyright Directive (EUCD) that is meant to solve the conflict between copyright exceptions and DRM, Article 6 (4) of the European Copyright Directive.

Christophe R., UFC Que Choisir / Warner Music

This latest case involved Christophe R. and UFC Que Choisir against Warner Music France and the music store Fnac. Christophe R. bought a CD by *Phil Collins*, "Testify", to discover later that he could not play it on his laptop, nor could he make copies from the CD. All this, according to Christophe R. and UFC Que Choisir, was because of some form of incorporated electronic copy protection. The plaintiffs' arguments – conflict with the "right to private copying" (since the decision of the Paris Court in 2004, it seems to have become standard among defendants of the consumer side, to refer to a "right to private copying", but then in quotation marks) and misleading behaviour – are familiar from earlier cases (see Tribunal Paris 2004, also Tribunal Bruxelles 2004). And again, the defendants insisted that UFC Que Choisir had no active legitimation to bring the case to court, that a right to private copying was non-existent, that the private copying exception would have to be interpreted in the light of the so-called three step test and, this is a new one, that informing consumers about the fact that burning the CD was impossible was futile as copying technology was in a state of constant flux – how could a decent producer keep track and label his products accordingly?

Thankfully, the Paris Court dealt rather curtly with the argument of a lack of legal standing of UFC Que Choisir (not accepted) and the argument of lack of playability (accepted). It then ventured, without further delay, bravely onto a terrain that causes grown-up politicians and law makers to mumble excuses, look in a different direction or at their shoes and do their best to change the topic. I am speaking of Article 6 (4) of the European Copyright Directive. Article 6 (4) of the European Copyright Directive is the provision in the European Copyright Directive that addresses the conflict between DRM and copyright's exceptions. I say "addresses" and not "solves", because all that Article 6 (4) of the EUCD does is to determine rather vaguely that "Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation … the means of benefiting from that exception or limitation."

Court says: Users of DRM have to respect private copying exception

The Tribunal de Grande Instance Paris, after having defended once again the private copying exception and explaining patiently why it was not in conflict with the three-step-test, stressed the need to interpret French law in the light of the European Directive (see already Court of Appeals, Paris, 2004). The court's interpretation of Article 6 (4) of the EUCD led it to the conclusion that technological protection measures must respect certain exceptions, including the private copying exception. With the understatement that is so characteristic of French judges, the court then expressed in a few words the essence of much scholarly writing and ranting over the past years by observing matter-of-factly: "the application of anti-copying protection devices by phonogram producers causes the statutory limitations of the authors' exclusive rights to authorise or prohibit reproductions to fade" ("La mesure de protection adoptee par le producteur du phonogramme fait disparaître la limite fixée par le législateur au droit exclusif de auteurs d'autoriser ou d'interdire la reproduction de leurs oeuvres"). Indeed.

The court continued with admirable straightforwardness to conclude that it is task of the DRM user, here: the phonogram producer, to make sure that private copying remains possible, despite the application of technological protection measures. In this point, it differed from the findings of the Court of Appeals in the "Mullholland Drive" case. There, the court did not read a principal obligation for rights holders to observe the private copying exception or any other exception in copyright law in Article 6 (4) of the EUCD. Consequently, the Appeals Court refrained from requiring compliance of DRM and the private copying exception, a matter that the court then left for the legislator. It restricted itself to postulate that 'the complete blocking of any possibilities of making private copies was an impermissible behaviour under French copyright law' (Court of Appeals, Paris 2005). In the Christophe R. case, the court was less hesitant and condemned Music Warner to refrain from using technological protection measures on "Testify" that do not allow for private copying. For each day of failure to comply with the order Warner Music will receive a monetary fine. In this concrete case, the conflict between TPMs and private copying was settled, at least for the time being (note: the case can still go on appeal).

Remains only the question what about all other CDs that are not by *Phil Collins*, produced by Warner Music, bought by Christophe R., called "Testify" and apply private-copying-hostile DRM? The decision of the Tribunal de Grande Instance has binding effect only between the parties immediately concerned. The answer can be read in Article 6 (4) of the EUCD: it is, indeed, up to parliament to settle the conflict.

Bottom line

Until now, France left it to its judges to face frustrated consumers and eloquent industry representatives and to sort out complaints about CDs or DVDs that would not play on a car radio, a PC, a laptop, and/or that could not be copied or ripped. French case law went through different phases: from a "no right to private copying" over explicit invitations to the legislator to take the matter into his hands, up to a ban on DRM that restrict private copying altogether. One thing is for certain: in the end the legislator will have to step in and face the matter. This is already because of the obligation in Article 6 (4) of the European Copyright Directive. So far, the pending proceedings in France to – finally – implement the European Copyright Directive into French law are not too promising. But this is yet another story…

Sources

- ► Helberger, Natali (2006): Vive la Balance! Pleading for a French revolution of copyright. INDICARE Monitor, Vol. 2, Numer 12, February 2006; http://www.indicare.org/tiki-read_article.php?articleId=181
- ► Senftleben, M. (2004): Copyright, Limitations and the Three-Step Test, Kluwer International, Den Haag, 2004
- ► Tribunal de Grande Instance de Nanterre (2003a): Tribunal de Grande Instance de Nenterre 6ème Chambre, judgement du 24 juin 2003, Association CLCV / EMI Muisc France, available at: http://www.legalis.net
- ► Tribunal de Grande Instance de Nanterre (2003b): Tribunal de Grande Instance de Nanterre 6ème chambre, judgement du 2 Septembre 2003, Francoise M. / EMI Music France, Auchan France, available at: http://www.legalis.net
- ► Tribunal Paris (2004): Tribunal de Grand Instance de Paris 3ème chambre, 2ème section, Stéphane P., UFC Que Choisir/Société Films Alain Sarde et, Judgement du 30 avril 2004, available at http://www.legalis.net

- Tribunal Bruxelles (2004): Tribunal de première instance de Bruxelles, L'ASBL Association Belge de Consommateurs TestAchats/SE EMI Recorded Muisc Belgium, Sony Music Entertainment (Belgium), SA Universal Music, SA Bertlesmann Music Group Belgium, SA IFPI Belgium, Judgement du 25 mai 2004, No. 2004/46/A du rôle de référes
- Court of Appeals (2005): Coud d'Appel de Paris 4ème chamber, section B, arrêt du 22 avril 2005, Stéphane P., UFC Que Choisir / Universal Pictures Video France et autres, available at: http://www.legalis.net

About the author: Natali Helberger is senior project researcher at the Institute for Information Law (IViR), Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and information services and the interface between technique and law, European media and intellectual property law. Ms. Helberger participates in the INIDCARE project as legal partner. Contact: helberger@ivir.nl

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=180

Vive la Balance!
Pleading for a French revolution of copyright

By: Natali Helberger, IViR, University of Amsterdam, The Netherlands

Abstract: This article reports about the French implementation of the famed Article 6 (4) of the European Copyright Directive, the article that orders member states to guarantee that consumers can benefit from exceptions despite the application of technological protection measures. Considering the fact that France is the origin of a series of groundbreaking decisions in favour of a balance between DRM use and consumer interests, figuring prominently among them the private copying exception, and all the public discussion those cases triggered, we have all reason to be curious about what the French legislator will come up with.

Keywords: legal analysis – copyright exceptions, copyright law, DRMS, EUCD, private copying, TPM - France

The awkward matter of DRM and copyright exceptions

There are probably few that would not agree that the anti-circumvention rules in the European Copyright Directive (EUCD) are a little tricky, if not to say awkward, or, let's be honest: simply not very well thought-through. Protecting right holders against greedy pirates may be a good and noble cause. Trouble is: the task of the copyright legislator is more complex than that. His task is, on the one hand, to protect and stimulate rights holders and, on the other hand, to promote the broad dissemination and use of works and to protect the public interest in works. Copyright law is a compromise between the economic and moral interests of right holders and public information policy interests in letting all of us benefit from creation and knowledge (Bard and Kurlantzick 1999). Though technological protection measures may, as some argue, benefit right holders in their battle against piracy, the reality is that the way technological measures are applied is often in conflict with cherished and broadly acknowledged principles of copyright law. The private copying exemption is one of these, to name but one, probably the most popular example.

Over the past three years important case law has evolved in France concerning the relationship between DRM users and consumers (cf. Helberger 2004, 2005a, 2005b, 2006). The French cases also informed lawyers, policy makers and academics outside of France. Having said that, the French decisions are binding only among the parties to the process, and cannot replace a more systematic approach to the conflict between DRM and copyright. To develop the latter is task of the French parliament, as the European Copyright Directive itself already states (in Article 6 (4) of the European Copyright Directive).

Copyright reform in France

As a matter of fact, that is exactly what the French Parliament is trying to do these months, in project Dadvsi (Le Project de Loi (N° 1206) relatif au droit d'auteur et aux droits voisins dans la société de l'information). Project Dadvsi serves the long-pending implementation of the EUCD, including, of course, the provisions about technological measures. Project Dadvsi took an interesting turn. Originally, the project was clearly destined to boost the legal position of the content industry, with proposals for the extensive protection of technological measures, draconic fines for file-sharers (jail up to three years), restrictions on the use of free software, mandatory obligations to implement DRM à la broadcasting flag, etc. Much to the horror of Minister of Culture Renaud Donnedieu de Vabres, the project then changed under the influence of massive external protests and some obstinate parliamentarians (socialists, who else) into a passionate discussion about guarantees for the private copy, legalising p2p networks and making interoperability of DRM mandatory. About 200 suggested amendments and lengthy heated discussions thwarted his initial plan to pass the law quietly and peacefully around Christmas 2005. Amendments suggested included interesting proposals like that technological protection measures should only be implemented with the knowledge/authorisation of the original author of that work (Amendment No. 84) or the suggestion to guarantee the private copying exception (Amendments No. 153 and 154). It remains to be seen which of these amendments will make it into the final bill. It would lead too far to discuss in this article all amendments, instead, we will concentrate on the transposition of the infamous Article 6 (4) EUCD in Article 8 of the draft law.

A French DRM-sarabande: One step to the front, five steps back

Article 8 of the draft law basically states that right holders will take initiatives to allow users to benefit from a private copying exception or an exception in favour of disabled persons. The rest of the draft article then concentrates on listing limitations to this obligation:

1. This only applies to consumers that have rightful access to the work (a provision that stems from the EUCD).
2. The obligation only applies in case the exception does not conflict with normal exploitation interests or legitimate interests of the author.
3. The right holder, furthermore, has the possibility to restrict the number of copies allowed.
4. The obligation does not apply to works that are made available on demand and at individual request, thereby excluding all download online services such as iTunes, movielink, etc…
5. And, finally, it is difficult to see how the obligation could be effective.

Why the present approach is a farce

The French legislator made the lion warden of the sheep. Admittedly, it seems a logical and fair step to burden users of DRM with the responsibility to make sure that the technology is applied in a way that respects the existing legal order. This was also the finding of the Tribunal the Grand Instance Paris. Having said this, any such obligation is of little value without accompanying measures that guarantee its enforcement (interesting, for the field of environmental law, see Börkey, P.; Glachant, M; Lévêque, F. 1998). Where the court imposed at least a daily fine in case of non-conformity, the draft law leaves a blank void. There is no deadline for the transition towards exception-friendly DRM, except a hazy rule that such initiatives would have to be taken "with a reasonable delay". Neither does the draft law foresee an independent body that would supervise the value and success of such initiatives to make DRM more exception-friendly. A vague reference is given that initiatives are made in agreement with interested parties. It is unclear who these interested parties are, if they must include representatives of consumer or public interests, what influence interested parties actually do have to bring in their interests effectively, etc.

Neither does Article 8 stipulate what shall happen if DRM users do not obey. According to the present draft: nothing. In the worst case, frustrated beneficiaries could take their case before the new arbitration body (that is to be created according to Article 9 of the draft law). The arbitration body can order DRM users to undertake initiatives necessary to benefit from an exception. Insofar, Article 9 of the French draft law resembles e.g. the Danish solution of a Copyright Tribunal (in § 75 d (1) of the Danish Copyright Act) (as to possible problems with this solution, see Foged 2004). Unclear is whether consumers (and consumer organizations) will still be able to bring DRM cases before courts, or whether they will in future have to file their complaints with the arbitration board first. In the latter case, the draft proposal might effectively set an end to a slowly but surely emerging body of case law in favor of consumer interests and DRM in France.

Equally problematic is the tendency that is expressed in the French draft as well as in the EUCD to protect the existence of exceptions in the offline environment, while accepting that they are overridden by technological measures and contracts in the online environment. It is difficult to see why the exceptions and limitations of copyright law should not apply in the online world. This is a technology-dependent approach that is likely to fail completely in the age of convergence. The fact that the danger of abuse is, as the argument goes, higher in an online environment does not alter the basic considerations about cultural exchange, freedom of expression, personal autonomy, information equality, etc. that have motivated the exceptions in the first place.

And even for the offline environment, the French draft law basically issues a charter to DRM users to override existing exceptions and limitations except the two mentioned in the draft Article 8: private copying and exceptions in favour of disabled persons. Why these two? In the public discussion around DRM and copyright exceptions, those are the ones discussed most loudly and that have, hence, the most political explosive potential. This, however, also demonstrates the danger of a too narrow discussion about DRM: important interests of the press, of artists, of libraries, universities and social institutions are too easily overlooked. For the protocol: the DRM-and-consumer-debate is not only about CDs and DVDs and private copying. It is about all kinds of digital content – text, news articles, books, games, film on or offline – and the various and diverse interests attached to its creation and dissemination.

It would seem that the Ministry of Culture is persistently trying to turn a deaf ear to the noise on French streets and in French courts. But France is in the national and international spot-lights: now is the time to act and to solve the conflict between DRM and copyright exceptions! Vive la balance!

Bottom line

Do we expect too much from France – every 217 years a new revolution (cf. Imhof 2005)? No, not at all. Over the past few years and thanks to the efforts of French consumer representatives, a public discussion has developed in France about DRM and consumers. This is a discussion that has influenced the way to look at DRM far beyond the borders of France. Creating the conditions for a more consumer-friendly DRM environment is not revolutionary – it is an increasingly widely acknowledged necessity for the functioning of the information society.

The basic approach being discussed presently in France in courts and parliaments – to hold DRM users liable for compliance with the law – is a hesitant step in the right direction. Liability alone however is not enough. Such an approach must be accompanied by measures that guarantee that DRM users take timely initiatives, and that such initiatives are effective and reflect the interests of all parties, including those of consumers.

Sources

- Bard, R. and Kurlantzick, L. (1999): Copyright Duration. Duration, Term Extension, The European Union and the Making of Copyrigth Policy, Austin & Winfield Publishers, San Francisco, 1999
- Börkey, P.; Glachant, M; Lévêque, F. (1998): Voluntary Approaches for Environmental Policy in OEDC Countries: An Assessment, online available at http://www.cerna.ensmp.fr/Documents/PBMGFL-OECDVAs.pdf
- Helberger, N. (2004): It's not a right, silly. The private copying exception in practice, INDICARE Monitor Vol. 1, No 5, 29 October 2004, available at: http://indicare.berlecon.de/tiki-read_article.php?articleId=48
- Helberger, N. (2005a): Thou shalt not mislead thy customer! INDICARE Monitor, Vol. 1, No 9, 25 Feb-February 2005, available at: http://www.indicare.org/tiki-read_article.php?articleId=76
- Helberger, N. (2005b): Not so silly after all - new hope for private copying, INDICARE Monitor, Vol. 2, No 6, 26 August 2005, available at: http://www.indicare.org/tiki-read_article.php?articleId=132
- Helberger, N (2006): Christophe R. vs Warner Music: French court bans private-copying hostile DRM. INDICARE Monitor, Vol. 2, Numer 12, February 2006; http://www.indicare.org/tiki-read_article.php?articleId=180
- Foged, T. (2004), Overview of implementation of the European anti-circumvention rules in Denmark, available at: http://www.euro-copyrights.org/index/4/11
- Imhof, P. (2005): Neues Urheberrecht in Frankreich, blog, 22. December 2005, available at: http://fippu.ch/).
- Le Project de Loi (N° 1206) relatif au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI), available at: http:// http://www.assemblee-nationale.fr/12/dossiers/031206.asp

About the author: Natali Helberger is senior project researcher at the Institute for Information Law (IViR), Amsterdam. She specialises in the regulation of converging media- and communications markets, electronic control of access to information and information services and the interface between technique and law, European media and intellectual property law. Ms. Helberger participates in the INIDCARE project as legal partner. Contact: helberger@ivir.nl

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=181

DRM beyond copyright enforcement – alternative models for content distribution

By: Daniel A. Nagy, Search-Lab, Budapest, Hungary

Abstract: In this article, we propose an alternative content distribution framework, which provides the necessary incentives for creating digital content without resorting to copyright enforcement. The proposed business model relies on peer-to-peer digital payment for which technical solutions already exist. Existing DRM technologies may actually be recycled for the purposes of the proposed business model, while removing the incentive misalignments currently plaguing the industry.

Keywords: economic analysis – business models, content distribution, digital payment, DRMS, P2P

Introduction

DRM (Digital Rights Management) has traditionally been thought of as a tool to enforce copyright. As such, it has failed spectacularly on several occasions (see e.g. Rubens 2002 about the DVD region code debacle or Orlowsky 2004 about the defeating of iTunes DRM). Practically every DRM solution with wide enough deployment for people to care was defeated within a short period of time.

In this article, we propose alternative business models which would provide the participating parties with the right incentives to do what other participants expect them to do, irrespectively whether or not copyright is enforced.

The proposed business models are based on several already successful business practices, which encourage creativity without relying on copyright protection. We strive to eliminate or minimize externalities by making sure that every participant is paid exactly for what they provide and pay exactly for what they get, while remaining in full control of whether or not to sell or buy services at a given price and are aware of the available alternative choices. Thus, the proposed business models can be expected to fare well in an unregulated free market.

Why does DRM fail as a tool of copyright enforcement?

The reason for this is that DRM is marred with severely misaligned interests of the concerned players:

1. Content authors, whose interests include compensation for their work, a loyal audience and wide publicity;
2. Publishers/distributors, whose primary interest is high revenue from content distribution;
3. Consumer electronics manufacturers, whose primary interest is high revenue from sales of devices;
4. Consumers, whose interests include low prices and a wide assortment of available content;
5. Governments, whose interests include high tax revenues, low enforcement costs, a reputation for enforcing laws and popular support.

DRM, in its traditional role as a tool of copyright enforcement, requires cooperation between authors, manufacturers, governments and publishers. In the light of the fact that devices with easily defeatable DRM sell better in an unregulated market, while implementing secure DRM is expensive, manufacturers need additional incentives to cooperate, such as government intervention and/or exclusive contracts (or even merger) with publishers/distributors. Also, manufacturers may choose to relocate to countries where such government intervention is smaller, thus providing governments with an incentive to defect from this cooperation. In addition, cooperation in copyright enforcement may erode the popularity of content creators, manufacturers and governments alike. The recent Sony-BMG case is an illustrative example of such backlash.

In such an environment, enforcing copyright in the face of extremely cheap, high quality alternative distribution channels (such as digital networks and recordable media) is a very difficult undertaking. On the other hand, content consumers have every reason to cooperate *against* copyright enforcement and can do so quite successfully, as has been observed with the widespread practice of burning CDs and DVDs for one another and the popularity of and considerable engineering effort put into peer-to-peer file-sharing and defeating DRM solutions.

For what are consumers prepared to pay?

As witnessed by the popularity of the otherwise quite expensive call-in and SMS votes on interactive television (such as those on Music Box, MTV and other commercial television channels), content consumers are prepared to pay for seeing their favourite content rank high in popularity ratings.

Such voting systems typically allow for multiple votes, precisely because voting requires financial sacrifice on the part of the voter, thus multiple voting is indeed indicative of higher commitment.

There is also evidence (see e.g. Madden 2004 about how artists perceive the issue) that consumers are quite willing to pay the author directly, even if the content is available for free from other sources. The more intermediaries are between the audience and the author, the more reluctant the former become to pay, if there are other means to get hold of the content.

Without going into moral or legal arguments, several surveys and other research suggest (see e.g. Madden 2004 and Dufft 2005) that the overwhelming majority of music consumers and authors (in sharp contrast with publishers) do not consider file-sharing as a major threat to the creative community. Most, however, do think that authors should be compensated.

Thus, it is reasonable to assume that people would be even more willing to pay for expressing their support for their favourite artists, knowing that most or all of the money they pay will go directly to the artist.

As recently as December, 2005, *Matt Philips* from the British Phonographic Industry (BPI) stated the following in an interview to BBC: "Download services would be far more popular if we gave all the music away for free. But of course we wouldn't have a business then – it's important that you charge for the product and that money can be re-invested in discovering new talent."

In the next section, we hope to address Mr. Philips' concerns in an innovative way.

Solutions for collecting and allocating such payments

Imagine a digital marketplace (e.g. a web- or mobile-portal) for content, where authors can offer their content, possibly with a short description and free samples for download in exchange for payment. All the payment is collected on accounts tied to corresponding pieces of content. There are no restrictions as to how much consumers can pay, except, perhaps a minimum price set by the author.

Content for sale is ranked according to the amount of money on these collector accounts. Thus, paying is essentially voting, informing other consumers about the popularity of the content. Authors can withdraw money from their accounts up to the accumulated balance. Thus, if they wish so, they can receive all the money their supporters paid. Alternatively, they can leave enough on the account to maintain or achieve high ranking.

In this model, the operators of such marketplaces are paid for exactly what they provide: discovering and evaluating talent. By being able to use the money left by authors on the collecting accounts, they essentially get access to interest-free credit. From their point of view, they get to sell their service at an auction price, which is the most they can hope for in a free market.

It is important to emphasize that ranking high does not directly increase or decrease the amount of money paid by supporters. We believe that the argument made in Fortunato (2005) applies to our system as well, which thus actually helps lesser known content providers (e.g. young artists) to attract attention and funding.

While, from a theoretical point of view, the proposed system works with unprotected content, DRM techniques can aid this business model by reducing the load on the operator; the operator in this case can sell only the rights, while the encrypted content itself is available for download from elsewhere, including peer-to-peer networks. In this case, DRM is not critical. If the minimal amount for getting the rights is lower than the effort required for defeating DRM, there is little motivation to attack it.

Another business model, which can even coexist with the previous one, is when customers are allowed to re-sell the content they have purchased at any price and in any quantity. In this case, the price customers will be willing to pay is considerably more than that of enjoying the content and voting for the artist; as it also includes the anticipated income from re-selling the content. Buyers who are also prospective sellers are interested in excluding free-riders, but protecting potentially very large files on storage and during transmission can be expensive. This is another point where DRM solutions can aid this business model: the content itself is available in encrypted form on web servers and peer-to-peer networks, but rights, including the decryption keys, are traded for money. Of course, the price will keep falling, but until it reaches a low level when protecting the content from non-paying consumers is not worth it any more, access to content will be kept restricted by those already accessing it. An extensive analysis of such a market is provided by Boldrin and Levine in their 2005 paper.

In both cases, it is instrumental to keep transaction costs as low as possible, as the transaction values on many occasions are very low. Both cash-like digital currencies with easy peer-to-peer payment and DRM solutions with small rights files enabling the use of large content files help reducing transaction costs to the point where the above outlined business models become viable.

Discussion

The proposed models are by no means restricted to music. The primary criteria for the applicability of the two proposed solutions are the following.

In the case, where payment also constitutes a vote for the content, the applicability depends on how the reputation of the author influences the demand for current and future work by the same author. It is an interesting question, whether or not such a system favours already popular content. While intuitively one would think that the proposed ranking scheme is biased against lesser-known authors and their works, such intuition is not necessarily justified (see Fortunato 2005 for a similar example). For instance, in an ordered list the difference between the attractiveness of the first and the second placed items does not directly depend on the actual difference between the amount of collected (and unused) funds. Another possible objection is that the proposed funding scheme does little to help the emerging artist to recoup the significant upfront costs of production. We believe that this is primarily a question of credit and the proposed system can be relied upon as a source of re-paying such credit. Furthermore, it allows the customers to credit the author directly, assessing the creditworthiness on the basis of past work.

In the second case, when content can be traded freely, the essential element for making the market efficient from both authors' and consumers' perspective is the extremely low distribution cost, which includes the transaction costs of payment. DRM solutions that reduce the cost of providing (and restricting) access from the need to transfer and store the whole content in a secure fashion to transferring and storing rights objects securely, which is orders of magnitude cheaper. Without DRM, these costs would be clearly prohibitive for high-quality video content, while introducing DRM would make it applicable to practically any kind of digital content ranging from poetry and simple still images to multiple hours of high-fidelity video (e.g. films). It is equally important for instantaneous payments to be possible and cheap. In the case of payments, even intangible costs like the effort and time required to make the payment become significant. This is one of the greatest challenges in making such a system feasible.

Bottom line

We have outlined two content distribution models, which do not depend on copyright and use DRM solutions to lower transaction costs while keeping transactions secure. Unlike the case of copyright enforcement, the proposed business models do not provide manufacturers and users of DRM-enabled devices (that is, those in the very best position to defeat DRM solutions) with incentives to actually sabotage and attack DRM.

They do, however, provide sufficient incentives to author and share creative content, which has historically been the role of copyright. While copyright was perfectly adequate in a world where transaction costs and copying costs were reasonably high, it is becoming increasingly controversial and difficult to enforce in a networked, digital world. In particular, DRM techniques regularly fail as copyright enforcement tools, primarily because of misaligned incentives. In the proposed business model, for which copyright is not relevant, DRM is a tool of lowering transaction costs together with a peer-to-peer digital currency.

Sources

- ► Boldrin, M. and Levine, D. K. (2005): Intellectual property and the efficient allocation of social surplus from creation. Review of Economic Research on Copyright Issues, 2005, vol. 2(1), pp. 45-66; http://levine.sscnet.ucla.edu/papers/rerci_revised.pdf
- ► Cullen, J. (2005): Music industry fails to stamp out digital piracy. BBC6 Today's Music News, Dec 5, 2005; http://www.bbc.co.uk/6music/news/20051220_download.shtml
- ► Dufft, N. (2005): Digital music usage and DRM. Results from a European consumer survey. INDICARE; http://www.indicare.org/survey

- Fortunato, S. et al. (2005): The egalitarian effect of search engines. arXiv.org, Nov 1, 2005; http://arxiv.org/abs/cs.CY/0511005
- Mackenzie, D. (2005): Soft cash in, hard cash out. New Scientist, 2005, issue 2509, pp. 40-43; http://www.newscientist.com/channel/info-tech/mg18725091.800.html
- Madden, M. (2004): Artists, musicians and the internet (survey findings). Pew Internet & American Life Project; http://www.pewinternet.org/pdfs/PIP_Artists.Musicians_Report.pdf
- Nagy, D. A. (2005): On cash-like digital payment systems, International Conference on Electronic Commerce and Telecommunication Networks, Reading, UK, Oct 3-7, 2005; http://www.epointsystem.org/~nagydani/ICETE2005.pdf
- Orlowsky, A. (2004): iTunes DRM cracked wide open for GNU/Linux. The Register, Jan 5, 2004; http://www.theregister.co.uk/2004/01/05/itunes_drm_cracked_wide_open/
- Rubens, P. (2002): Border controls crumble in DVD land. BBC NEWS dot.life, Aug 19, 2002; http://news.bbc.co.uk/1/hi/in_depth/sci_tech/2000/dot_life/2197548.stm

About the author: Daniel A. Nagy is an information security expert, interested in financial cryptography and the economics of cyberspace. Currently, he works for SEARCH-LAB Ltd, Budapest. He is also the lead developer of ePointSystem.ORG.

Status: first posted 15/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=172

The Future Digital Economy: A session report on DRM

By: Philipp Bohn, Berlecon Research, Berlin, Germany

Abstract: On January 30th and 31st, the Organisation for Economic Co-Operation and Development (OECD) and the Italian Minister of Innovation and Technology, *Lucio Stanca*, invited delegates from all OECD countries to Rome. Several speakers were scheduled to discuss digital content creation, distribution and access. One panel specifically addressed “Content diffusion: IPR, DRM, licensing, content security, standards”. This article summarizes some key ideas and statements, primarily concerning DRM.

Keywords: conference report - business models, digital content, interoperability, IPR, media, standards

Introduction

During the conference a wide range of success factors for the digital economy was discussed: availability of broadband access was stressed as a crucial prerequisite for most business models, the importance of amateurization – enabled by cheap ways to produce and alter digital content and make it available through the Internet – was introduced by *William Fisher* (Director, Berkman Center of Intellectual Property Law) in his dinner speech and was picked up by several speakers later on. Convergence of media and services was another trend identified, threatening established players and giving opportunities to new market entrants that profit from low barriers to entry – think e.g. of Voice over IP. Public sector information was another important topic opening new business perspective. The BBC for example is starting to make older documentaries and movies available to the public via the Internet.

There is apparently no easy answer to the role of governments and their agencies confronted with these rapid developments. One fundamental policy issue however coming up again and again across panels and plenary sessions was the need for a fair balance in intellectual property rights including DRM. For instance *Toyoda Masakazu* (Director-General, Japanese Ministry of Economy, Trade and Industry) called for an unbundling of the operating and DRM systems to prevent the emergence of monopolies (Apple and Microsoft are trying to strengthen their market position using their respective DRM systems). *Rita Hayes* (Deputy Director General, Copyright and Related Rights and Industrial Relations, WIPO) suggested a common approach to DRM standards, especially regarding device- and content-interoperability. *Michael Geist* (Professor, Canada Research Chair in Internet and E-commerce Law, University of Ottawa), suggested that content companies from the movie and music industries should reduce their reliance on DRM – a practice that "locks down" content (cf. Geist 2006).

In the following this report will concentrate on the panel dedicated to DRM and related issues. The mere fact that a special session on these issues took place is another indicator of the importance of IPR and DRM for the future of the digital economy.

Panel discussion on DRM

The following persons were asked to join the panel (in order of appearance): Marco Ricolfi (Professor, University of Turin, Law School) as the panel's chair, Stan Liebowitz (Professor, Center for Analysis of Property Rights and Innovation, University of Texas), Leonardo Chiariglione (CEO and Digital Media Strategist, CEDEO.net), Fred von Lohmann (Senior Intellectual Property Attorney, Electronic Frontier Foundation), Giorgio Assuma (President, Italian Collecting Society SIAE), Barney Wragg (Senior Vice President eLabs, Universal Music Group International) and Sarah Deutsch (Vice President and Associate General Counsel, Verizon Communications).

Marco Ricolfi introduced the topic by pointing out the long and the short route of content distribution. Traditionally, there has been a large number of intermediaries between producers and consumers. While intellectual property rights as well as technological infrastructure is tailored to the long route, with digital distribution there might also be shorter decentralized routes between producer and consumer. As chairman of this session Ricolfi put in further interesting arguments in the course of this afternoon. He picked up e.g. the phenomenon of amateurization and called for the new IPR rules to be compatible with this type of content. Touching on the debate on the copyright term, he considers it to be too extensive, often hindering innovation (e.g. in case of software development). A further question worth considering was in his view, whether DRM-based solutions will alter the role of collecting societies that traditionally represent artists' rights.

Stan Liebowitz's introductory presentation focused on "Promises and Threats of the Digital Economy". Digital distribution is a very efficient way of distribution, which continues to have a significant impact on the music industry. However, consumers are adapting only hesitatingly to commercial channels: While in 2003 2% of the record industry's revenue was derived from online sales, this figure was still only 5% in 2005. Liebowitz specifically blamed rampant P2P use for the slow uptake of commercial offerings and called for further support from the side of governments.

Leonardo Chiariglione lamented about the "miserable state of debate" concerning digital media and rights management. He made an important distinction between "enforcement" and "management" of digital rights. While DRM by nomenclature should be rights management, it is in most cases the enforcement of rights. As such, it reduces economies of scale, and is often difficult to manage due to its proprietary nature. Although a "DRM conversion box" for incompatible DRM systems might offer some relief, no such technology has been embraced in a significant way. Also, proprietary DRM systems' lack of interoperability lowers the profitability of the whole digital value chain. In his view, only an open DRM standard as put forward by the Digital Media Project (DMP) offers a viable alternative. Part of "Plan B", what Chiariglione called a "liberating message", is the idea that each stakeholder in the market can decide individually on the level of protection.

Fred von Lohmann warned that using the terms "consumers" and "customers" or even "stakeholders" is framing the discussion about usage rights and protective measures in a way that is not desirable. The discussion should rather be about what "fans" or "the public" want. It is accepted for various other online services that success comes with the ability to deliver a "cool user experience".

However, this appears to be a minority opinion when it comes to digital content distribution. In particular, incompatible DRM systems limit content usability and accessibility.

But there is also great opportunity in digital content distribution, such as sharing content and experiencing community. This was possible only to a very limited degree with physical media such as CDs, which von Lohmann referred to as “frozen cultural artifacts”.

Being a copyright lawyer by training, he stressed that innovative technologies like cable TV or VCR could only be developed and introduced to the market due to gaps in intellectual copyright law, not thanks to tight legislation. He proposed that intellectual property law should be interpreted generously during the early developmental stages of the digital economy. New legal regulations should be formulated ex-post, reflecting the actual evolution and the proven need of regulation. That's what he proposed as his “Plan B”.

To get an idea of what consumers expect to do with content, decision and policy makers are well advised to go to places where people “don’t know any better” and “innovate anyway”, such as the blogosphere and other amateur sites. This could give guidelines as to how laws should be drafted or technology and business models be developed.

Giorgio Assuma maintained that also in the age of digital distribution, artists need to rely on collecting societies. Without them, it would be impossible to efficiently manage and protect digital rights. He pointed out that this could be done in a more transparent way, due to technological developments.

As a representative of a major record label, *Barney Wragg* expressed some annoyance about constant accusations from certain stakeholders in the digital economy. Rather than hindering market developments, record labels are actively promoting them with new business models – for example made-for-mobile content, portable subscriptions, licensed P2P networks as well as on-demand services based on advertising revenue. Virtually every major label has built up its own digital label, releasing songs via the Internet rather than on CDs.

According to Wragg, his label has two main objectives: One was to offer many profitable services, the other was the protection of artists’ intellectual rights. Limiting factors for the success of digital distribution are lack of DRM interoperability as well as inflated financial expectations from participants along the value chain, especially on the side of mobile operators.

Sarah Deutsch praised the importance of the Digital Millennium Copyright Act (DMCA) and the WIPO (World Intellectual Property Organization) treaties for digital content production and distribution.

With communication providers trying to move up the value chain, content is of utmost importance for Verizon. The company’s on-demand video offering, FiOS, delivers content encrypted end-to-end, in order to curb infringement.

When infringement is detected within Verizon’s network, the company sends a warning note to the offending user. Content providers (e.g. Disney) are not notified about this act, as a measure to safeguard customers’ privacy. Only in case of continued violation of copyright law the user faces contract termination.

However, it is only a matter of time until consumers “wake up” to the limits of DRM. This means that all companies on the digital economy’s supply side have a considerable responsibility to balance user interests and the protection of intellectual property.

For example, customers might experience frustrations caused by DRM when they migrate to a new mobile phone. Verizon made the effort to educate its customers that no songs would be lost if they backup their licenses. Deutsch called for standardization of DRM systems and expressed the hope that non-interoperable DRM systems might one day be referred to “that recent unpleasantness”.

Bottom line

The Conference helped to address frictions, discuss possible solutions and also prepare for future developments of a dynamic digital economy. Attitudes towards DRM as an efficient means to protect digital content vary significantly. While major content providers tend to stress the importance of deploying such technical protection measures, smaller stakeholders and activist groups point out risks and obvious challenges. It would have been interesting to also hear a representative from one of the major consumer electronics manufacturers or technology providers, such as Apple, Sony and Microsoft, who are often blamed for not engaging in the deployment of interoperable DRM standards.

Sources

- Conference website with more information on the conference, presentations and webcasts: www.oecd.org/sti/digitalcontent/conference
- Geist, Michael (2006): Locking down our digital future. BBC news, 8 February 2006; http://news.bbc.co.uk/1/hi/technology/4690188.stm

About the author: After having graduated from University of Mannheim (Business Administration), Philipp Bohn joined Berlecon Research as Junior Analyst in 2005. He is a member of the INIDICARE-team. Contact: pb@berlecon.de

Status: first posted 20/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=173

Research into user-(un)friendly DRM. A review

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The study *privacy4DRM* reviewed here offers on the one hand a noteworthy contribution to conformance testing of DRM systems with respect to privacy, and on the other hand a harsh criticism of traditional business models relying on DRM systems combining copy protection and personalisation of content. Perspectives of new consumer-oriented business models combined with user-friendlier technical solutions are sketched.

Keywords: review – business models, consumer expectations, data protection, DRMS, music markets, privacy, technology assessment, user-friendliness

Introduction

The German Ministry for Education and Research (BMBF) established a line of research funding called "Innovation and technology analysis" (ITA). The publication reviewed here is the outcome of such a sponsored project on DRM (cf. ITA-BMBF). Project partners were the Fraunhofer Institute for Digital Media Technology (IDMT), a data protection agency (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), and a university (Technical University Ilmenau). The title *privacy4DRM* tells about the *main* focus of the project: to investigate privacy with respect to existing e-commerce platforms relying on DRM systems. The cases analysed are:

- Apple's iTunes (Fairplay),
- T-Online's Musicload (Windows Media Rights Manager - WMRM),
- Sony's Connect-Europe (OpenMG),
- Bevision-Shops (based on the PotatoSystem), and
- Adobe's Digital Media Store (PDF).

In addition to the techno-legal privacy analysis performed, the study also attempts to provide a broader explanation why the dominant business model in online music markets based on strong DRM does not work.

In the following the review will present first the structure of the study, second the main findings of the privacy analysis, and third the main arguments of the more general reasoning. Finally we will discuss the findings. As the study (Bizer et al. 2005) is in German, I will also draw on two related articles in English (published in the Axmedis proceedings: Grimm 2005, and Will 2005). A short article by Bizer et al. (2006), which resumes the study in 6 pages, has also been considered for this review.

Overview of the study

Chapter 1, the introduction, explains the objective of the study: to come up with a catalogue of criteria for user-friendly and privacy-conforming DRMS, to be applicable not only to the music market, but also to other markets like the educational market. In the introduction you also find an outline of the legal framework of privacy and copyright.

Chapter 2 on "methodology" sets out the legal, economic and technical criteria to be applied, and sketches how the interdisciplinary analysis was performed. On the one hand data flows and traces were tracked down and checked if they conform with the criteria of privacy. On the other hand the economic analysis of the download platforms addressed the value propositions for consumers, the revenue and business models of the content providers, and transaction costs from both points of view, the consumers' and the businesses'.

Chapter three to seven describe the 5 services chosen (see above) and present the findings of the different analyses one by one. Chapter 8 gives an overview of these findings.

Chapter 9 called "mission" contains what might be better termed "conclusions", as the findings are discussed here at a general level addressing policy issues, and proposing more consumer orientation and more user-oriented DRM systems design.

The last chapter is titled "recommendations for action". The first part of this chapter discusses if and how the results derived from the music market can be applied to the areas of education, learning, and research. While the same rules may apply for e-learning materials such as books, music, and video, interactive learning tools clearly need different types of access and usage control comparable to those for computer games and interactive software (Bizer et al. 2005, p. 204f).

The second part of chapter 10 comes up with six topics deserving further research: (1) new distribution models and new services are still lacking appropriate protocols and infrastructure concepts; (2) new distribution models for digital libraries, educational publishing, and research publications are particularly challenging in this respect; (3) economic research on incentive models for new distribution models is needed; (4) comprehensive risk management of DRM-systems is still lacking; (5) it is still an open question how to implement pseudonymity concepts in DRM systems and how to legally frame them, and finally (6) the idea of "privacy labels" (Datenschutzgütesiegel) is put forward.

DRM and privacy

The most innovative aspect of the study is in my view its scrutiny of data flows taking place and data traces being produced when using DRM systems. In order to analyze DRM systems, the authors use a privacy model which is in line with the European data protection directive (EU 1995; Grimm 2005, p.108) and also conforms with corresponding national regulations. The result of this analysis is that state-of-the-art DRM systems "collect more personal data from their customers than necessary to fulfil the purchase service. There are many hidden interfaces, both by encoding personal data within the products, and by linking clickstream data with contractual data" (Grimm 2005, p. 112).

Even if knowledge about customers may be used exclusively to improve the service, the fact that e-content providers hide their actions to consumers, shows a lack of trust, which in turn leads to a lack of trust on the consumers' side when they become aware of this. A particularly disturbing finding is the encoding of personal data within digital products. This action is again intransparent to the customers. In other words, forensic DRM, meant to trace illegal behaviour, is added to the DRM system. As the authors put it: "… most shop systems which use DRM, do not trust the built-in mechanisms of DRM to enforce the usage rules in the end-user devices. Therefore they use the trace method as a second line of defense. They collect data to identify users, not only for business purposes, but also to link products to their buyers in order to identify the origin of products in illegal environments." (Grimm 2005, p. 108; Bizer et al. 2005, p. 198). The good news if you like: there was no proof that the investigated systems collect data about individual usage patterns. If this were the case it would clearly violate existing privacy legislation (Bizer et al. 2005, pp. 183, 192).

A pro-active, transparent policy by the content providers involving the consumers could alleviate the situation to a certain extent. The situation could be further improved by implementing pseudonymity options, as many marketing purposes don't require information about the persons using a service (Bizer et al. 2005, p. 200). A third measure proposed to increase trust are "privacy labels" guaranteeing that the DRMS is respecting privacy. This approach might be highly interesting for those in favour of conformance testing like the Transatlantic Consumer Dialog (cf. their DRM declaration with respect to privacy; TACD 2005).

Assessing "state-of-the-art" DRM systems

As stated above the study also aims to assess what they call "state-of-the-art" DRM systems in the context of music markets. I will try to boil down their reasoning to 10 points.

1. No doubt, a balance is needed between the right of creators to obtain remuneration for their creative work, and the interests of end-users and the public.

2. In the currently dominating business model content is to be sold analogue to physical goods, i.e. as a digital object. DRM is meant to enable the old business model by protecting the digital object.

3. In order to achieve this, "classical" DRM couples content, client, and device (Bizer et al. 2005, p. 181). To get access to purchased content, the end-user now has to legitimize himself or herself to the digital object. Furthermore DRM systems add data collection to copy protection. On top, as a second line of defense, forensic DRM using personal data is added to strong copy protection (p. 188, 191). As an important aside the authors argue, that assuming personalisation of content (forensic DRM) is already a matter of fact, the request of content providers to get a right to get personal information from the ISP appears excessive and unnecessary (p. 182).

4. The way DRM systems are designed and implemented is contrary to a basic principle of IT-security, namely that the party interested in the protection must have the means to enforce the protection. This is difficult in the case of DRM systems, because the mechanisms to enforce the protection are located on the end-user's side. Ultimately he or she is sovereign of the computing device (p. 17). Cooperation can not be expected and circumvention is a reality – in particular if the value proposition for end-users is poor.

5. The lack of acceptability of protected content is due to at least three shortcomings of current DRM systems:

- ► (1) immature technology excluding even uses foreseen by the providers (e.g. playing a CD at home and in the car; p 197f),
- ► (2) DRM systems not respecting either fair use or allowing for the copyright exceptions granted by law (p.197), and
- ► (3) non-interoperable technology putting the burden on the consumers having to implement and purchase multiple tools and devices to get what they want (p. 197).

6. The lack of acceptability of protected content is due also to a defective trust relationship between business and consumers. Forensic DRM, when performed in an intransparent way, and anti-piracy campaigns criminalizing customers undermine trust.

7. The authors assert that existing music download platforms using DRM-systems are in reality not a success (p. 193-195) – not even iTunes.

8. Consumers are supposed to decide whether to purchase legal content on the basis of an transaction cost calculus. "The customer is willing to pay for the avoidance of expected transaction costs when downloading illegally. He is not willing to pay for the usage of the data" (Will 2005, p. 99).

9. Within the current paradigm the situation can be improved, if DRM systems are de-

signed conforming to privacy principles, with increased end-user involvement, more user-friendly design, and with greater interoperability.

10. However this cure might not be enough and alternative business models and revenue models need to be developed, focussing on services. People would be willing to pay for added value (recommendations, preview etc.). Users might also accept collection of personal data if they get in turn more individualised services. Content providers should actively involve end-users providing them with more options and choice what usage rights to obtain. Under these conditions, new services based on "user-oriented DRM" (p. 199) are more likely to be accepted.

Discussion

While old DRM seems to be the illness it purports to cure (adapted from *Karl Krauss*, the Austrian writer's famous sentence about psychoanalysis), new user-oriented DRM seems the healthy way out. By and large I share the reasoning presented, and indeed INDICARE has always pointed to the shortcomings of the old business model and the potential of new business models (cf. e.g. INDICARE 2004). However I would like to add six remarks to enrich the picture drawn by the authors.

1. With respect to transparency and user involvement requested, when it comes to data collection and privacy, I would go even further and stress the potential of combining DRM and PET (privacy enhancing technology) as Korba and Kenny (2002) have done in their seminal paper "Towards meeting the privacy challenge: Adapting DRM" (cf. also Tóth's introduction to Privacy Rights Management (PRM) in the INDICARE Monitor 2004).

2. I would not underline that legal download platforms can't be a commercial success. Although the IFPI:06 Digital Media Report's message "legal online buying is catching up with illegal file-sharing" contains a considerable portion of wishful thinking, the strategy of the music industry combining law suits against P2P file sharing services, legal actions against individual uploaders (ca. 20.000 in 2005, cf. IFPI 2006, p. 18), threatening campaigns, deteriorating quality of content on filesharing servers, and improving their own offerings in terms of scope and interoperability should not be underestimated. There is no *a priori* that the big players of the music industry *must* fail.

3. I can imagine new service oriented offerings ruled by somehow transparent DRM. I can also see that these might be perceived as a "fair deal", thus increasing the acceptance of those services. But would this change the basic flaw of DRM as pointed out by the authors themselves, namely that DRM systems are not in line IT-security principles (see point 4 above)?

4. While I see the potential of new business strategies where you pay for added-value and not for content, I doubt if this model does justice to creators, and I am afraid that this approach might also help to erode the foundations of copyright and creative works.

5. An important reason why consumers behave illegally and why people feel so uncomfortable with DRM is not mentioned. Restrictions imposed by DRM violate the consumers' sense of ownership. The intuitive understanding of "property" is linked to ideas such as long term possession, unlimited use and the right to resell. Remember Thomas "If men define situations as real, they are real in their consequences" (the so called Thomas theorem). The fact that property rights with respect to digital goods imply a change from ownership to rights of disposal (licensing) is obscured even by the content industries themselves - still suggesting that you buy music when you pay for it. This argument has been elaborated in an INDICARE Monitor article about the mind-set of pirates(Böhle 2005).

6. The authors introduce type of *homo oeconomicus* who calculates transaction costs when looking for content (see point 8 above). This argument has to be differentiated based on the previous remark, and furthermore because empirical research tells us that consumers are willing to pay for content itself if the payment (or a considerable share of it) goes to the creators themselves (cf. Madden 2004; see also Regner and Barria 2005).

Consumer behaviour is obviously more value-oriented than expected. You may play the David-Goliath-game, while at the same time respecting creators. Research into piracy (see point above) also indicates that the social reputation to be gained from savvy filesharing within groups is rather important.

Bottom line

The most innovative aspect of the study is in my view its scrutiny of data flows taking place and data traces being produced when using DRM systems, combined with concrete ideas on how to improve the situation: by transparency, pseudonymity options, and "privacy labels". The general reasoning on DRM has very strong points like the contradiction between DRM systems and IT-security. Consumer behaviour, however, seems to be modelled in a too abstract fashion disregarding social factors.

Sources

- Bizer, Johann; Grimm, Rüdiger; Will, Andreas (2006): Privacy4DRM: Nutzer- und datenschutzfreundliches Digital Rights Management. DuD • Datenschutz und Datensicherheit ,30 (2006) H 2, pp. 69-73
- Bizer, Johann; Grimm, Rüdiger; Möller, Jan; Müller, Michael; Müller, Anja; Jazdzejewski, Stefan; Puchta, Stefan; Will, Andreas (2005): Privacy4DRM, Datenschutzverträgliches und nutzungsfreundliches, Digital Rights Management, Kiel/Ilmenau; http://www.datenschutzzentrum.de/drm/privacy4drm.pdf
- Böhle, Knud (2005): About the mind-set of software pirates. INDICARE Monitor; Vol. 1, Number 8, January 2005; http://www.indicare.org/tiki-read_article.php?articleId=74
- EU (1995): Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
- Grimm, Rüdiger (2005). Privacy for Digital Rights Management Products and their Business Cases. In: Nesi, Paolo; Ng, Kia; Delgado, Jaime (eds.) (2005): Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, IEEE Computer Society, pp. 107-112.
- IFPI (2006): IFPI:06 Digital Music Report; http://www.ifpi.org/site-content/library/digital-music-report-2006.pdf
- INDICARE (2004): Helberger Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report, Amsterdam, December 2004; http://www.indicare.org/soareport
- ITA-BMBF: http://www.innovationsanalysen.de/de/projekte/digital_rights.html
- Korba, Larry and Kenny, Steve (2002): Towards Meeting the Privacy Challenge: Adapting DRM. NRC paper number NRC 44956, November 2002, http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44956.pdf
- Madden, M. (2004): Artists, musicians and the internet (survey findings). Pew Internet & American Life Project; http://www.pewinternet.org/pdfs/PIP_Artists.Musicians_Report.pdf
- Regner, Tobias and Barria, Javier (2005): Magnatune – A voluntary-based model for online music. INDICARE Monitor, Vol. 2, Number 8, October 2005; http://www.indicare.org/tiki-read_article.php?articleId=147
- TACD (Transatlantic Consumer Dialogue) (2005): Resolution on Digital Rights Management http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=275; or http://www.tacd.org/db_files/files/files-380-filetag.doc
- Tódt, Gergely (2004) DRM and privacy - friends or foes? An introduction to Privacy Rights Management (PRM). INDICARE Monitor; Vol. 1, Number 4, September 2004; ;http://www.indicare.org/tiki-read_article.php?articleId=45
- Will, Andreas (2005): An economic analysis of music download platforms: Proceedings of the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, IEEE Computer Society, pp. 97-100

About the author: Knud Böhle is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led

various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, knud.boehle@itas.fzk.de

Status: first posted 22/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=174

Informed consumers should welcome the implementation of *effective* DRM – if it meets their needs

By: Mark Bide, Senior Consultant, Rightscom Limited, London, United Kingdom

Abstract: The need to protect intellectual property is part of a much wider – and increasingly urgent need – to implement a wider framework of "digital policy management" on the network. Consumers will not only accept digital policy management but will welcome it – so long as it is designed to meet their requirements and expectations, not simply to defend the existing business models of today's media and technology businesses.

Keywords: opinion – civil society, consumers, copyright exceptions, policy management, DRMS, e-commerce, trust, trusted computing

Introduction

We must seek out a new approach to managing trust on the network.

To date, our halting attempts at cobbling together a "digital rights management" solution have been at best unconvincing, at worst completely inept – because they have been exclusively focused on protection of intellectual property rights, and have approached the issue in a very limited way. What we now call "DRM" needs to evolve into something which perhaps we will come to call "Digital Policy Management" – a new technical approach to managing trust on the network.

Some of the policies we want to manage in this way may indeed be rooted in intellectual property rights protection. But others will stem from personal or corporate policies (like privacy and confidentiality); yet others may come from interpretation of the legal code. Effective protection of intellectual property – in a manner that is acceptable to consumers – should be a side effect of this new "Digital Policy Management" approach to managing trust, not the main event.

Building a framework for network citizenship

The challenge of maintaining a framework for protection of intellectual property on the network is closely related to many other challenges which are facing us on the network. Despite the best efforts of both lawmakers and of those who would enforce the law, users bent on using the internet with felonious intent persistently stay one step ahead. Fraud is rife, and fraudulent emails become ever more sophisticated. Attempted extortion based on denial of service attacks has recently been exemplified by the attack on "Million Dollar Homepage" (cf. Gonsalves 2006). Although the recent attack of the Kama Sutra virus may not have been as disastrous as predicted (BBC 2006), viruses and spyware continue to proliferate throughout the network. And spam, while perhaps exemplary of a rather different level of malfeasance, creates a problem for every user of the network that is – in its totality – immensely costly.

At first sight, these "network citizenship" issues may appear to have little link with intellectual property and digital rights management, but the problem in all these cases is one of trust and trusted identity.

Our response to the attack on trust on the network has been somewhat feeble. Trust circles, like those based on "friend of a friend" (cf. sources) linking of personal web pages – or more business oriented approaches like LinkedIn (cf. sources) – undoubtedly have a role to play; but they don't deal with the problem of the outside world, with the fact the Internet is (as I have recently seen it described; Becker 2006) a "world of strangers" – nor with the reality that those strangers are not universally benign. To move beyond this world of strangers, we need to move from concepts like trust circles to more robust mechanisms that allow us to truly trust one another's assertion of identity and to grant appropriate permissions to those that we do trust.

Renewing trust on the Internet

In a recent article (Talbot 2005), *David Clark* of MIT, an Internet pioneer, is quoted as saying: "We might just be at the point where the utility of the Internet stalls – and perhaps turns downward" – because of the growing loss of trust. The economic and social implications of a widespread loss of trust in the network are incalculable; it is now integrated into our lives at a very deep level.

In a similar vein, *Vint Cerf*, one of the "founding fathers" of the Internet, and now Google's "chief internet evangelist" was recently quoted (Talbot 2006) as saying: "I believe the potential growth of the Internet will be limited if we allow invasive badware and spyware to continue to fester without strong action. All consumers must be in control of their experiences when they browse the Internet and the mass proliferation of badware threatens this control. We cannot allow that to continue…. The providers of Internet services and software simply must get this problem under control."

You do not necessarily need to share the view that we urgently need a complete re-engineering of the fundamental architecture of the Internet to recognise that there is real enough problem to address. Nor is it necessary to accept uncritically the architecture proposed by the Trusted Computing Group (TCG; cf. sources), which appears to run the risk of putting an excessive amount of power into the hands of a small number of technology companies. In the circumstance, the words "trust", "trusted" and "trustworthy" can all become a little slippery.

No one will easily be brought to trust technology solutions which threaten "lock in" to particular providers of technology, and to hand power to a technocracy.

Avoidance of lock in is dependent on interoperability and low switching costs, something that the TCG proposals could impose considerable limitations on. Interoperability is therefore the key challenge – and interoperability will depend on the availability "policy metadata": clear, unambiguous and standardised ways of *expressing* policies – in many ways, building this layer of policy data is a much more significant task than *enforcing* the policies.

Indeed, the ability to express the policies in a standard, interoperable way provides us individually with options – options as to whether policies are to be enforced through technology (in the context of intellectual property, think "DRM") or through a combination of trust, good will and the law (think "Creative Commons").

Of course, there is potential downside to the interpretation of essentially *uncertain* legal concepts into the *certainty* of machine-interpretable code. It becomes necessary to hard code concepts of "reasonableness" and "proportionality", things that are by their nature contextual. This inevitably creates a challenge in areas like exceptions to copyright; but we should face up to those challenges rather than simply spike them as "too difficult".

Maintaining the balance

We do well to remember that copyright was established for the good of society: "To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries" (US Constitution). Technology should no more be used to extend the intended scope of copyright protection than it should be used to destroy its central purpose.

There can be few who still doubt that the internet will prove to be a hugely disruptive technology for the copyright industries, just as it proving hugely disruptive for other sectors. However, before deciding that we want to dispose of the entire structure of intellectual property, we should be sure that we have fully considered the consequences.

Ultimately, effective management and protection of intellectual property on the network will only be possible within a framework of trusted (and trustworthy) network computing. However, the primary motivation for the implementation of such a framework will not be the protection of the current business models of the media and technology industries (who have not always acted in ways guaranteed to make themselves popular with consumers).

Consumers will welcome the introduction of digital policy management technology – including management of “digital rights” – only if it also offers a solution to *their* underlying security and identity problems and contributes to the maintenance of civil society on the network, with all the complex checks and balances that this implies. This will not easily be achieved, but that does not mean that it is not worth the effort.

Sources

- BBC news (2006): "Limited" damage from Nyxem virus. BBC News 3 February 2006; http://news.bbc.co.uk/1/hi/technology/4677022.stm
- Becker P. (2006): A world of strangers” The Digital ID World Newsletter 2 February 2006; http://www.digitalidworld.com/modules.php?op=modload&name=News&file=article&sid=318
- Gonsalves, A. (2006): "Million Dollar Homepage" targeted in huge denial-of-service attack. Information Week 13 January 2006; http://www.informationweek.com/news/showArticle.jhtml?articleID=177100372
- LinkedIn: https://www.linkedin.com/
- Talbot, D. (2005): The Internet is broken” Technology Review 19 December 2005; http://www.technologyreview.com/InfoTech-Networks/wtr_16051,258,p1.html
- Talbot, D. (2006): Google, Sun Backing New Anti-Malware Effort” Technology Review 25 January 2006; http://www.technologyreview.com/InfoTech-Software/wtr_16184,300,p1.html?PM=GO
- The Friend of a Friend Project: http://www.foaf-project.org/
- Trusted Computing Group: https://www.trustedcomputinggroup.org/home
- US Constitution, Article 1, Section 8: http://www.archives.gov/national-archives-experience/charters/constitution_transcript.html

About the author: *Mark Bide* is a Senior Consultant at Rightscom Limited, a specialist consultancy based in London which was founded in 2000 to support the design and deployment of business, technology and process solutions in the management, protection and trading of intellectual property rights and content in the digital environment. Mark has over 30 years experience in the publishing industry, having been a Director of the European subsidiaries of both CBS Publishing and John Wiley & Sons. With a background in production, distribution, and publishing technology, he has been a consultant for nearly 15 years and has particular expertise in the impact of network technology on the information value chain. He has been closely involved in standardisation strategies to support the management of intellectual property on the network. Contact: mark.bide@rightscom.com

Status: first posted 22/02/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=175

Trusted computing for digital rights management

By: Robert A. Gehring, Computers and Society, Technical University, Berlin, Germany

Abstract: The relationship between trusted computing (TC) systems and digital rights management (DRM) systems is discussed. Trusted systems technology was developed in the 1960s, while the modern concept of DRM is a brainchild of the Internet era of the 1990s. While TC technology can be used to build DRM systems, both belong to different categories and should not be confused. TC technology may as well be deployed to protect "darknets" (Biddle et al. 2003) for sharing data. Making TC-based "copyright boxes" (Stefik 1999) is by no means a guarantee for business success in marketing digital content where consumer demand is ignored.

Keywords: technical analysis - consumer expectations, copyright boxes, darknets, DRMS, trusted computing, trusted systems

Introduction

First things first. No, trusted computing (TC) is not the same as digital rights management (DRM). DRM technology has been built, and will be built in the future, entirely without relying on TC support. And yes, DRM can be based on TC technology, as Chinese PC maker Lenovo has just demonstrated (cf. Dornan 2006).

According to Information Week, Lenovo’s latest ThinkPad model uses a fingerprint sensor in combination with a trusted platform module chip (TPM) and software support from Microsoft and Adobe for controlling access to, and distribution of, PDF documents (Dornan 2006). Lenovo’s DRM approach ties biometrics, content (i.e., documents), and TPM support, in order to enforce usage rights and monitor actual use of the content. Accessing a "controlled" PDF document first requires authentication through fingerprint identification; without authentication, access is denied. The creator of the document is the one who determines who subsequently may access the PDF. The Lenovo system is also prepared to track acts of accessing and reading the document, and reporting this information. Whether the TPM plays a key role in the scenario is unclear as of now.

Depending on your standpoint, Lenovo’s innovation may be "particularly frightening" (Dornan 2006) or a good thing. And that exemplifies the crux of trusted computing in general: What is good use or evil use depends on purpose and positioning. In itself, trusted computing is merely a tool, as recently pointed out by Linux kernel developer *Alan Cox*: "There's a lot of political debate, that it's really evil or good. But it's only a tool" (Marson 2006). Those who use this tool with intention will decide on its meaning.

Although TC technology has primarily been propagated for security improvement of networked end systems, multiple observers were quick to point out that some of its basic features were similar to mechanisms that allow supporting DRM. In some extreme cases, TC has literally been equated with DRM; this is, as a thinly veiled attempt to introduce ubiquitous control mechanisms on formerly open PC architectures.

As a tool for making the behaviour of computer systems more predictable, by enforcing rules on users and processes (i.e., mandatory access control), trusted computing creates ample opportunity for ruling out undesirable effects of software – and software users. At the same time it empowers parties controlling access to the rule-making process to forcing users to comply with their private interests, and to cut out competitors, when attempting to access, and use, system resources. Whether any such attempt will be successful in the long run is contingent on economical and political factors as well.

As the latest Sony-BMG debacle with the XCP and MediaMax copy protection software has shown, misjudgements of consumer expectations can easily lead to costly backlashes, and even to legal and legislative action (Helberger 2006; Leyden 2006; and see the documentation at Groklaw 2006). Hence, the price of using digital rights management - be it based on trusted computing technology or not - may be higher than the price of foregoing access control in the first place. And as *David Pakman*, CEO of eMusic.com, emphasised, the logic of DRM is not necessarily good business logic, too: "If it were possible to demonstrate that non-DRM'ed music encourages more sales, wouldn't it make sense for the industry to offer portions of its catalog as unrestricted MP3 files? It seems like bad business to bind every category of customer and every category of product with the same sales offering" (Pakman 2005).

While TC technology may be helpful in "hardening" DRM systems, it is in no way helpful for selling music beyond demand. And if systems are almost impossible to crack, and that it is what TC promises to do, governments are highly concerned (Stone-Lee 2006). And from a content-owners point of view, trusted systems built on TC technology, in fact may well turn out as a nightmare. A network of trusted systems could be used to establish a technically impenetrable file sharing community, a TC-protected darknet (for darknets see Biddle et al. 2003).

So when discussing the relationship between DRM and trusted computing, one has to keep in mind that not everything that is technologically feasible is economically viable or politically acceptable at the same time.

This article discusses in short the relationship between DRM and trusted computing, and what makes TC technology useful for implementing DRM. For practical reasons, it is not possible here to delve into details of TC technology. Instead, the interested reader is referred to (Pearson et al. 2003; Smith 2005).

"Trusted computing is DRM": Dispelling a myth

Learning some facts about the history of trusted computing and DRM might be helpful in distinguishing the relative merits of either concept.

Historically, trusted computing has its roots in the concept of trusted systems (Kuhlmann and Gehring 2003). Trusted systems are neither new nor invented by the Trusted Computing Group (TCG), the body behind the most important TC architecture. Actually, research on trusted systems dates back to the 1960s. Efforts were driven by government and military needs for effective protection of information in the cold war era. Two research approaches proved particularly influential:

- The reference monitor (RM) concept introduced in 1973 by *James Anderson* (Anderson 2001, p.140); and
- The Bell–LaPadula (BLP) model as introduced in the same year by *D. Elliott Bell* and *Leonard J. LaPadula* (Anderson, Stajano and Lee 2001, p.189).

While Anderson’s reference monitor has been conceived as a proposal for governmental establishments, BLP was developed for a military environment with well-defined security requirements.

BLP was primarily designed to deal with restricting the information flow between formally distinguished security levels and compartments. The RM concept, on the other hand, models a system architecture suitable to enforce arbitrary access control policies. It can be regarded as a container to be filled with a rule set of choice. As such it is pretty generic and flexible - "an abstract machine that mediates all accesses to objects by subjects" (Bishop 2003, p.502).

Once filled with an access control policy, i.e. specific rules for access control, a reference monitor will enforce that policy. A validated, tamper-resistant implementation of a RM forms the policy-core of a trusted system, its so called trusted computing base (TCB), and "consists of all protection mechanisms within a computer system - including hardware, firmware, and software - that are responsible for enforcing a security policy" (Bishop 2003, p.502).

Note the interplay of “hardware, firmware, and software” making the trusted system work. One important but often overlooked property of the *trusted system concept* is its policy-neutrality; it was not designed as a DRM concept (see below). In practice, however, *concrete trusted systems* will enforce specific policies. It depends on all three factors – “hardware, firmware, and software” – which access control rules will be enforced. In other words, hardware vendor, firmware vendor, and those who provide and configure the system’s software stock, will set the rules. Conceptually, trusted systems are as able to enforce DRM policies as they are to enforce “mandatory open-access” (think of a system that refuses to create files with access control attributes).

TCG (former TCPA) and trusted systems

Founded in 1999 by Compaq, HP, IBM, Intel, and Microsoft, the Trusted Platform Computing Alliance (TCPA) was relaunched in 2003 as the Trusted Computing Group (TCG). As of January 2006, the TCG had more than 120 members.

The TCG’s mission is to "develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms" (Trusted Computing Group 2006). It does not provide hardware or operating system software.

TCG specifications exist so far for:

- Infrastructure Specifications
- PC Client Specifications
- Trusted Platform Module (TPM) Specifications
- Trusted Network Connect (TNC) Specifications
- TPM Software Stack (TSS) Specifications
- Server Specific Specifications

The one outstanding advantage the industry-wide approach of the Trusted Computing Group has to offer for building trusted systems is that it *standardises components*. TC enables mass-production of hardware components and reuse of software components, thus making it comparatively cheap to build trusted systems.

From trusted systems to DRM

Digital rights management (DRM) is a relatively new development going back to the 1990s. *Mark Stefik*, researcher at Xerox’s Palo Alto Research Center, promoted the idea of "usage rights management" (Stefik 1996a, p.221) – a term much more appropriate to describe what DRM does – for digitally distributing intellectual property. He located the root of the problem of selling content in the architecture of modern personal computer systems: "Fortunately, computers need not be blind instruments of copyright infringement. Properly designed digital systems can be more powerful and flexible instruments of trade in publications than any other medium. The seeming conflict between digital publishing and commerce is merely a consequence of the way computer systems have been designed to date." To overcome this “design flaw,” he suggested using "techniques for commerce in what we call digital property rights or usage rights…several kinds of rights besides copying" (Stefik 1996a, p.221). That comes close to what DRM systems do today.

What is a DRM system?

Although, there is no single one definition for what constitutes a DRM system, the modern conception regards three elements as crucial (Rump 2003):

- Technology;
- Law; and
- Business Model.

The business model is this: keeping supply of certain binary data short and charging for metered access to this artificially “scarce resource”. Technology is applied to protect this business model for marketing binary data by controlling access to, and usage of, while legal protection for technological measures discourages circumventing technological barriers to otherwise free access to data. Due to very liberal laws, there is no need for the data to represent “works of authorship” under copyright protection, and it is not hard to find an old movie, the copyright of which has expired, to be nevertheless distributed on DVD with CSS copy-protection.

The only perfect DRM system is one that can neither be broken nor avoided. And while this article focuses on the technology side, that statement refers to all three elements of DRM: If one of the three elements can be broken or avoided, the DRM system is doomed to fail.

Different approaches for implementing DRM have been broken and the content they guarded leaked onto the Internet. Thus, people had alternative ways of access to content and could avoid using DRM systems. Legal threats were no real show-stopper (IFPI 2006).

What makes TC technology especially attractive for implementing DRM is their ability to enforce usage policies. Once their security conditions are broken, TC systems stop working. Since their security conditions are built as a "chain of trust" containing hardware-locked keys and certificates from trusted third parties, they are hard to tamper with, at least much harder than software-only systems. Being able to rely on a trusted system, it is a fairly simple thing to implement a hard-to-break "usage rights management" as the platform of choice for content owners.

Coming DRM-enabled operating systems, such as Microsoft's Windows Vista flavours, are aimed at providing "casual, honest users with guidelines for using and consuming content based on the usage rights that were acquired" (*Dan Glickman*, President of the Motion Picture Association of America, in BBC 2006). That is necessary, because "[w]ithout the use of DRMs, honest consumers would have no guidelines and might eventually come to totally disregard copyright and therefore become a pirate" (ibid.). To reinforce the guidelines, trusted computing features are deployed (see the Lenovo example in the introduction), all the more appealing if components are cheap (see above).

Selling copyright boxes

Rather than modifying their age-old control-based model of making money from copyrighted works, the content industries pursued DRM as their one and only salvation from having to suffer "the fate of the buffalo" (Bronfman 2000, quoted in Fridman 2000).

The idea of using concepts developed for trusted systems as blueprints for "usage rights management" systems was widely promoted by Stefik. He argued that "the first key to commerce in digital works is to use trusted systems" (Stefik 1996a, p.228) – and apparently he was quite persuasive. Turning general-purpose computers, or special-purpose devices, into "vending machines" thus enabling potential customers "to order digital works any time of the day and get immediate delivery" (Stefik 1996a, p.228), sounded like a huge business opportunity. Transforming computers hitherto under the control of their users (often being their owners, too) into "copyright boxes" (Stefik 1999, p.55) more like radios, TV-sets, and CD-players – this idea really took off with content industries seeking to commercialise the internet after the ban on commercial activities was lifted in the middle of the 1990s.

But a DRM system is almost useless, that is from a content owner's perspective, until it is deployed broadly. Putting together cheap TC components with a market-dominating operating system "enriched" with DRM functionality is the most economic way to provide the majority of users with "copyright boxes." Microsoft is doing just that (Microsoft 2006).

Bottom line

TC technology is neither necessary nor sufficient to implement DRM but it can make implementing DRM easier and cheaper. TC components are tools – neither good nor bad. It's the way the tools are used, the interplay of "hardware, firmware, and software," that gives them meaning. And predictably, software will have the biggest part in the play, defining most of the functionality. People are using trusted systems to do things. One way to use trusted systems is to build DRM systems. But there is no way to guarantee success for DRM systems. DRM may well turn out to be "[m]edia companies' next flop" (CNET 2006) if consumer expectations are not met. And consumers want to get what, when, where, and how, they like it, without the hassle of incompatible devices. Just like in the file sharing networks.

Sources

- Anderson, R.J. (2001): Security engineering: A guide to building dependable distributed systems. New York: Wiley.
- Anderson, R.J., Stajano, F., Lee, J. (2001): Security policies. In: Advances in Computers, Vol. 55, pp 185-235
- BBC (2006): Digital film: Industry answers. In: BBC Entertainment, 09 February 2006, http://news.bbc.co.uk/1/hi/entertainment/4691232.stm
- Becker, E., Buhse, W., Günnewig, D., and Rump, N., eds. (2003): Digital rights management: Technological, economic, legal and political aspects, Lecture Notes in Computer Science, Vol. 2770, Berlin, Heidelberg, New York: Springer.
- Biddle, P., England, P., Peinado, M., and Willman, B. (2003): The darknet and the future of content protection. In: Becker et al. (2003), pp. 344-365
- Bishop, M. (2003): Computer security: Art and science. Boston, MA: Addison-Wesley
- Bronfman, Jr., E. (2000): Remarks as prepared for delivery by Edgar Bronfman, Jr. Real Conference 2000, San Jose, CA, May 26, 2000 (a copy of the text of the speech can be found at http://seclists.org/lists/politech/2000/May/0068.html)
- CNET 2006: DRM: Media companies' next flop? In: CNET News.com, 30 January 2006, http://news.com.com/DRM+Media+companies+next+flop/2030-1069_3-6032936.html
- Dornan, A. (2006): Yes, trusted computing is used f or DRM; Information Week, 17 February 2006, http://www.informationweek.com/blog/main/archives/2006/02/yes_trusted_com.html
- Fridman, S. (2000): Firm thinks it can solve music-pirating problem. ComputerUser.com, 31 May 2000, http://www.computeruser.com/news/00/05/31/news2.html
- Groklaw (2006): Sony DRM; http://www.groklaw.net/staticpages/index.php?page=20051122010323323
- Helberger, N. (2006): The Sony BMG rootkit scandal; INDICARE Monitor, Vol.2, Numer 9, January 2006, http://www.indicare.org/tiki-read_article.php?articleId=165
- IFPI (2006): Digital Music Report 2006. http://www.ifpi.com/site-content/library/digital-music-report-2006.pdf
- Kuhlmann, D. and Gehring, R.A. (2003): Trusted platforms, DRM, and beyond. In: Becker et al. (2003), pp 178-205
- Leyden, J. (2006): Homeland security urges DRM rootkit ban; The Register, 17 February 2006, http://www.theregister.co.uk/2006/02/17/rootkit/
- Marson, Ingrid (2006): Trusted computing comes under attack; ZDNet UK, 27 January 2006, http://news.zdnet.co.uk/internet/security/0,39020375,39249368,00.htm
- Northrup, T. (2006): Windows Vista security and data protection improvements. Microsoft, 01 June 2005, http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx
- Pearson, S., Balacheff, B, Chen, L., Plaquin, D., and Proudler, G. (2003): Trusted computing platforms: TCPA technology in context. Upper Saddle River, NJ: Prentice Hall.
- Pakman, D. (2005): Why DRM everything? A sensible approach to satisfying customers and selling more music in the digital age; Groklaw, 31 December 2005, http://www.groklaw.net/article.php?story=20051231013858642
- Rump, N. (2003): Digital rights management: Technological aspects. In: Becker et al. (2003), pp 3-15
- Smith, S.W. (2005): Trusted computing platforms: Design and applications. Berlin, Heidelberg, New York: Springer.
- Stefik, M., ed. (1996): Internet dreams: Archetypes, myths, and metaphors. 3rd Printing 2001, Cambridge, MA: The MIT Press.
- Stefik, M. (1996a): Letting loose the light: Igniting commerce in electronic publication. In: Stefik (1996), pp 219-253.
- Stefik, M. (1999): The internet edge: Social, technical, and legal challenges for a networked world. Cambridge, MA: The MIT Press.
- Stone-Lee, O. (2006): UK holds microsoft security talks. BBC, 16 February 2006, http://news.bbc.co.uk/1/hi/uk_politics/4713018.stm
- Trusted Computing Group, https://www.trustedcomputinggroup.org/home

About the author: *Robert A. Gehring* is a computer scientist specialising in issues of open source, intellectual property, and information security. He is an associate researcher with the research group for Computers & Society at the Technical University of Berlin and editor of the

iRights.info consumer information website. He is co-editor of the German open source annual *Open Source Jahrbuch* and can be contacted via rag[insert at sign here]cs.tu-berlin.de.

Status: first posted 01/03/06; licensed under Creative Commons; to be included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=179

OpenTC – an open approach to trusted virtualization

By: Dirk Kuhlmann, Hewlett Packard Laboratories, Bristol, UK

Abstract: Due to the increasing complexity of IT systems, the mutual attestation of platform characteristics will become a necessity for proprietary as well as Open Source based systems. Trusted Computing platforms offer building blocks to achieve this goal. Their combination with non-proprietary virtualization technology can help to avoid much feared negative side-effects of Trusted Computing. It will permit to run locked-down execution environments in parallel with unconstrained ones, making it possible to support tight security requirements while maintaining user choice. An open approach to Trusted Computing is a prerequisite for future community based effort to describe and attest expected properties of software components in a trustworthy manner.

Keywords: project description – open source, security, trusted computing - EU

Introduction

The advent of "Trusted Computing" (TC) technology as specified by the *Trusted Computing Group* (cf. sources) has not met much enthusiasm by the Free/Open Source Software (FOSS) and LINUX communities so far. Despite this fact, FOSS based systems have become the preferred vehicle for much of the academic and industrial research on Trusted Computing. In parallel, a lively public discussion between proponents and critics of TC has dealt with the question whether the technology and concepts put forward by the TCG are compatible, complementary or potentially detrimental to the prospects of open software development models and products.

Common misconceptions of TC technology are that it implies or favours closed and proprietary systems, reduces options of using arbitrary software, or remotely controls users' computers. It has long been argued, though, that these and similar undesirable effects are by no means unavoidable, not least because the underlying technology is passive and neutral with regard to specific policies. The actual features displayed by TC equipped platforms will almost exclusively be determined by the design of operating systems and software running on top of it. With appropriate design, implementation and validation of trusted software components, and by using contractual models of negotiating policies, negative effects can be circumvented while improving the system's trust and security properties. This is the intellectual starting point of the EU-supported, collaborative *OpenTC* research and development project (project Nr. 027635; cf. sources) that started in November 2006.

Combining FOSS and TC technology

OpenTC aims to demonstrate that a combination of TC technology and FOSS has several inherent advantages that are hard to meet by any proprietary approach. Enhanced security at the technical level tends to come at the expense of constraining user options, and the discursive nature of FOSS-development could help to find the right balance here. Trusted software components have to be protected from analysis during runtime, so it is highly desirable that their design is documented and that the source code is available to allow for inspection and validation. Finally, any attempts to introduce TC technology are likely to fail without the buy-in of its intended users, and openness could prove to be the most important factor for user acceptance.

OpenTC sets out to support cooperative security models that can be based on platform properties without having to assume the identifiability, personal accountability and reputation of platform owners or users. For reasons of privacy and efficiency, these models could be preferable to those assuming adversarial behaviour from the outset. A policy model based on platform properties, however, requires reliable audit facilities and trustworthy reporting of platform states to both local users and remote peers. The security architecture put forward by the TCG supplies these functions, including a stepwise verification of platform components with an integral, hardware-assisted auditing facility at its root. In *OpenTC*, this will be used as a basic building block.

Trusted virtualization and protected execution environments

The goal of the *OpenTC* architecture is to provide execution environments for whole instances of guest operating systems that communicate to the outside world through reference monitors guarding their information flow properties. The monitors kick into action as soon as an OS instance is started. Typically, the policy enforced by it should be immutable during the lifetime of the instance: it can neither be relaxed through actions initiated by the hosted OS nor overridden by system management facilities. In the simplest case, this architecture will allow to run two independent OS instances with different grades of security lock-down on an end user system. Such a model with an unconstrained "green" environment for web browsing, software download / installation and a tightly guarded "red" side for tax record, banking communications etc. has recently been discussed by Carl Landwehr (2005). More complex configurations are possible and frequently needed in server scenarios.

OpenTC is borrowing from research on trusted operating systems that goes back as far as 30 years. The underlying principles – isolation and information flow control – have been implemented by several security hardened versions of Linux, and it has been demonstrated that such systems can be integrated with Trusted Computing technology (see e.g. Maruyama et al. 2003). However, the size and complexity of these implementations is a serious challenge for any attempt to seriously evaluate their actual security properties. The limited size of developer communities, difficulties of understanding and complexity of managing configurations and policies continue to be road blocks for deployment of trusted platforms and systems on a wider scale.

Compared to full-blown operating systems, the tasks of virtualization layers tend to be simpler. This should allow *OpenTC* to reduce the size of the Trusted Computing Base. The architecture separates management and driver environments from the core system and hosted OS instances. They can either be hosted under stripped-down Linux instances, or they can run as generic tasks of the virtualization engines. The policy enforced by the monitors is separated from decision and enforcement mechanisms. It is human readable and can therefore be subjected to prior negotiations and explicit agreement.

OpenTC chose (para-)virtualization as the underlying architecture for a trusted system architecture, which allows to run standard OS distributions and applications side by side with others that are locked down for specific purposes. This preempts a major concern raised with regard to Trusted Computing, namely, that TC excludes components not vetted for by third parties. The *OpenTC* architecture allows to limit constraints to components marked as security critical, while unconstrained components can run in parallel.

OpenTC builds on two virtualization engines: XEN and L4. Both are available under FOSS licenses and boosted by active developer and user communities. Currently, it is necessary to compile special versions of Linux that cooperate with the underlying virtualization layer. However, the development teams will improve their architectures to support unmodified, out-of-the-box distributions as well. This will be simplified by hardware support for virtualization as offered by

AMD's and INTEL's new CPU generations. Prototypic results have shown that this hardware support could also allow to host unmodified operating systems other than Linux (see e.g. Shankland 2005).

From trusted to trustworthy computing

TCG hardware provides basic mechanisms to record and report the startup and runtime state of a platform in an extremely compressed, non-forgeable manner. It allows to create a digitally signed list of values that correspond to elements of the platform's Trusted Computing Base. In theory, end users could personally validate each of these components, but this is not a practical option. End users may have to rely on other parties to evaluate and attest that a particular set of values corresponds to a system configuration with a desired behaviour. In this case, their reason to trust will ultimately stem from social trust he puts in statements from specific brands, certified public bodies, or peers groups.

A much discussed dilemma arises if trusted components become mandatory prerequisites for consuming certain services. Even in case such components are suspicious to the end user, they might still be required by a provider. This problem is particularly pronounced if named components come as binaries only and do not allow for analysis. The recent history of DRM technology has shown that trojans can easily be inserted under the guise of legitimate policy enforcement modules. Clearly, a mechanism that enforces DRM on a specific piece of content acquired by a customer must not assume an implicit a permission to sift through the customer's hard disk and report back on other content.

This highlights an important requirement for components that deserve the label "trusted": at least in principle, it should be possible to investigate their actual trustworthiness. A clearly stated description of function and expected behaviour should be an integral part of their distribution, and it should be possible to establish that they do not display behaviour other than that stated in their description – at compile time, runtime, or both. A socially acceptable approach to Trusted Computing will require transparency and open processes. In this respect, a FOSS based approach looks promising, as it might turn openness into a crucial competitive advantage.

The TCG specification is silent on procedures or credentials required before a software component can be called "trusted". *OpenTC* works on the assumption that defined methodologies, tools, and processes to describe goals and expected behaviour of software components are needed. This way, it will become possible to check whether their implementation reflects (and is constrained to) their description. Independent replication of tests may be required to arrive at a commonly accepted view of a component's trustworthiness which in turn requires accessibility of code, design, test plans and environments for the components under scrutiny.

Trust, risk, and freedom

Most of us have little choice but to trust IT systems where more and more things can go wrong, while our actual insight in what is actually happening on our machines gets smaller by the day. Users are facing a situation of having to bear full legal responsibility for actions initiated on or by their machines while lacking the knowledge, tools and support to keep these systems in a state fit for purpose. Due to the growing complexity of our technology, we will increasingly have to rely on technical mechanisms that help us to estimate the risk prior to entering IT based transactions. Enhanced protection, security and isolation features based on TCG technology will become standard elements of proprietary operating systems and software in due time.

This evolution is largely independent of whether FOSS communities endorse or reject this technology. *OpenTC* assumes that mutual attestation of the platforms' "fitness for purpose" will become necessary for proprietary systems as well as FOSS based ones. The absence of comparable protection mechanisms for non-proprietary operating or software systems will immediately create problems for important segments of professional Linux users. In fact, many commercial, public or governmental entities have chosen non-proprietary software for reasons of transparency and security. These organizations tend to be subjected to stringent compliance regulations requiring state-of-the-art protection mechanisms. If FOSS based solutions don't support these mechanisms, the organizations could eventually be forced to replace their non-proprietary components with proprietary ones: a highly undesirable state of affairs that *OpenTC* might help to avoid.

From this perspective, the current discussion about the next version of the GNU public license raises serious concerns. Some of the suggested changes could impact the possibility to combine Trusted Computing technology and Free Software licensed under GPLv3 - this refers to the GPLv3 Draft, status 2006-02-07 16:50 (cf. sources). Section 3 of this draft concerns *Digital Restrictions Management*, a term that has been used by Richard Stallman in discussions about Trusted Computing. For example, the current draft excludes "*modes of distribution that deny users that run covered works the full exercise of the legal rights granted by this License*". It is an open question whether this might apply to elements of a security architecture such as *OpenTC*. A Trusted Computing architecture does not constrain the freedom of copying, modifying and sharing works distributed under the GPL. However, it can constrain the option running modified code *as a trusted component*, since previously evaluated security properties might have been affected by the modifications. Unless a re-evaluation is performed, the properties of modified versions can not be derived from the attestation of the original code; security assurances about the original code become invalid.

This is by no means specific to the Trusted Computing approach; it also applies to commercial Linux server distributions with protection profiles evaluated according to the Common Criteria. The source code for the distribution is available, but changing any of the evaluated components results in losing the certificate. Whether or not software is safe, secure, or trustworthy is independent of the question of how it is licensed and distributed. The option to choose between proprietary and FOSS solutions is an important one and should be kept open. This is one of the reasons why several important industrial FOSS providers and contributors participate in *OpenTC*. The project aims at a practical demonstration that Trusted Computing technology and FOSS can complement each other. This is possible in the context of the current GPLv2. Whether it will be so under a new GPLv3 remains to be seen.

Sources

- GPLv3 Draft, status 2006-02-07 16:50: http://gplv3.fsf.org/draft
- Landwehr, Carl (2005): Green Computing. IEEE Security&Privacy, Vol 3, Nr 6, Nov/Dec 2005, p. 3
- Maruyama et al. (2003): Linux with TCPA Integrity Measurement. IBM Research Report RT0575, January 2003; http://www.research.ibm.com/trl/people/munetoh/RT0507.pdf
- OpenTC: http://www.opentc.net
- Shankland, Stephen (2005): XEN passes Windows Milestone. CNET News.com, August 23, 2005; http://news.com.com/Xen+passes+Windows+milestone/2100-7344_3-5842265.html
- Trusted Computing Group: http://www.trustedcomputinggroup.org

Disclaimer

The content of this paper is published under the sole responsibility of the author. It does not necessarily reflect the position of HP Laboratories or other OpenTC members

About the author: Dirk Kuhlmann is a senior research engineer for Hewlett Packard Laboratories in Bristol, UK, where he works as a member of the Trusted Systems Laboratory. He acts as the overall technical lead for the OpenTC project. Contact: dirk.kuhlmann@hp.com

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=183

The role of Trusted Computing in Digital Rights Management within the OpenTC project

By: Florian Schreiner, Michael Pramateftakis and Oliver Welter, Institute for Data Processing, Munich University of Technology, Munich, Germany

Abstract: Much of the negative impression of DRM comes from the fact that current systems offer very little transparency and convenience to the user. Within the OpenTC project, we pursue an approach for DRM towards the introduction of a standardised license-processing core that is open to the public and common to a variety of DRM-related applications. We hope that the trusted environment, in which the DRM core and applications are executed, together with the open architecture, will help to introduce clarity and convenience in the DRM process and thus give a positive spin to the topic.

Keywords: technical analysis – DRMS, MPEG-21, OMA, Trusted Computing

Introduction

Digital Rights Management (DRM) systems govern the use of content by describing per-user rights in machine-readable licences and enforcing them by using cryptographic methods. The public's conception of the term "DRM" today does not extend beyond a copy-protection system of the content industry. DRM systems are seen as means to just restrict copying and sharing of multimedia content and are thus viewed negatively.

The OpenTC project will provide an open-source framework for establishing trusted application environments on free operating systems like Linux. This approach plans to enforce integral trust and security of the system, because the applications are caged in trusted environments, in which only certified, trustworthy applications are allowed to run. The system can detect malicious software like viruses and exploits and prevents their execution. Furthermore, OpenTC protects imperilled programs against external access, so that no program outside the environment may access security relevant data. The trust is rooted on a Trusted Platform Module (TPM), a hardware component that can securely store cryptographic keys and ensure integrity of the system.

We aim to use this concept for creating a DRM system which governs the use of all kinds of sensitive data, not just multimedia content. An example for alternative uses of DRM is the medical sector, where patient records and related information have to be protected against unauthorised access. Without a trusted environment, attackers may enter a computer system e.g. by using a virus or exploiting a security vulnerability to obtain unauthorised access to stored information, including sensitive data. In a trusted system, sensitive information is protected by encryption. The corresponding keys are stored within the TPM and are bound to a specific platform state (This procedure is called "sealing" in the Trusted Computing Group nomenclature). Rogue software is never allowed to be executed in a trusted system and even if it were, it would alter the platform's state, thus disabling access to the "sealed" keys.

A trusted infrastructure on an open-source system may open the door for devising DRM systems providing two primary advantages: Transparency and interoperability. By introducing an open DRM core that is common to all applications, the DRM procedure becomes more transparent. This is in strong contrast to the current situation, where security is mainly based on obscurity, i.e. on keeping the function of the DRM system itself secret. This leads to proprietary applications to handle protected content and as a direct consequence thereof those applications preclude interoperability. Accordingly, many different systems and applications exist for performing the same task, each one having its own ways for managing content and licenses. In contrary to that, an open architecture facilitates interoperability, because the DRM core uses standardised technology for license management. Various elements of the MPEG-21 standard will be used to accomplish this mission. Internally, the DRM core works with MPEG-21, so whenever licenses from external licensing domains are introduced to the system, e.g. licenses issued by OMA DRM or Windows Media DRM, the DRM core translates them into an equivalent MPEG format so it can manage them. Such translations, although technically feasible, are facing trust problems. Since licenses are signed by the content owners or rights holders, a translated license must also be signed by a trustworthy entity. Such a signature is only possible when a trusted environment is present, like the one provided by OpenTC. The trusted environment is also beneficial in cases where content reencryption is needed.

MPEG-21 Rights Expression Language (MPEG REL) is a language versatile enough to accommodate functionality from various other rights expression languages. Thus, translations to and from other languages are possible, as long as they are based on the same principles. Such translations are needed when content needs to be transferred to external devices for rendering. The procedure can be made transparent to the user, who does not have to deal with trust issues, as they are automatically taken care of by the DRM core.

A concept for an interoperable DRM system

Our concept is based on several services that we can expect from the OpenTC infrastructure: The TPM-Chip is the root of trust in the system and is used by OpenTC for building up a trusted environment for applications. Only certified applications are allowed to run in such a context and they can rely on the fact that the underlying operating system with its modules and drivers are trusted, too. We assume that all data within the secure environment is protected against attacks, so no special care or encryption in the user layer is necessary any more. The distributor of the operating system decides which program is secure and which not, and provides relevant certificates. These certificates may also contain information about the capabilities of the application or the level of security it needs to perform particular actions. Depending on this information, OpenTC can restrict access to sensitive information or specific hardware components of the system. Thus, uncertified applications, including viruses, manipulated hardware drivers and other malicious code cannot start in a secure environment. This protection is transparent to the user, as the OpenTC infrastructure takes care of it in the background without the need for user intervention.

The diagram next page shows our currently planned architecture with the above environment in mind:

The central component of the system is the DRM-Core. Its tasks are to offer several services to the application layer regarding interpretation of licenses, as well as to provide the central key store for protected content. As it is a component used by several applications, it is placed within the OpenTC infrastructure. That way, it can be certified along with the system and be trusted by all applications. The Core consists of three basic parts: The license parser, the translation manager and the key store.

License Parser

The License Parser offers services regarding verification and interpretation of licenses. These services are central to any DRM process and are accessed from the outside by an API, which includes all functions that are necessary for an application to access a protected file. A player application can be any program that can be executed in a trusted environment and that is able to render content. It has to be compatible to the DRM-System to know the API of the core and how to handle content. Such a player application can directly access the DRM-Core via the API to request access to protected content. The player has to provide its license, so the core can decide if the user has permission to access the data. If access is granted, the core returns the content key from the key store and the player can render the content. Legacy players, which cannot access the API directly, are also supported by our architecture. Players of that kind are not aware of the DRM-Core, but are favoured by users for whatever reason. These cases are handled by an IO-Socket interface, which handles the license authentication and interpretation transparently to the application. For the player, the whole process is similar to a normal file access. The player only has to support the content's type and be connected to the IO-Socket through a plug-in. The player receives the unprotected content from the socket and can render it. The IO-socket in this case converts and forwards requests through the API to the DRM-Core. Since all applications, including the legacy ones, run in the secured environment, handing out the content key or the decrypted content itself is no problem, since it is guaranteed that the applications will not misuse it. This is a great advantage of having a trusted computing base.

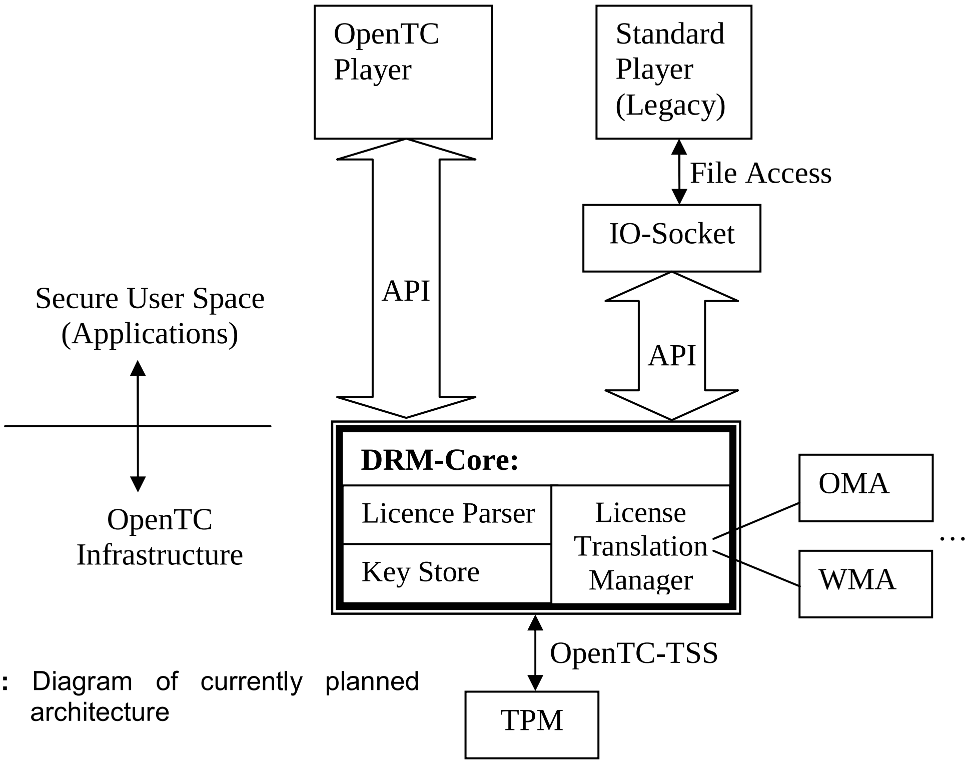

Figure 1: Diagram of currently planned architecture

License Translation Manager

Internally, the core uses MPEG-21 as a DRM framework. MPEG-21 also provides facilities for identifying content. Unique identifiers are used by the core to relate content with licenses and keys in the key store. Whenever foreign content enters the system, i.e. content protected with a license in a language other than MPEG REL, the license translation subsystem converts the external license to MPEG REL, so that it can be processed by the license parser. Since the core is trusted, the translation can also be trusted. The license translator uses an extensible architecture which utilises plug-ins for different license formats. Our prototype will support at least OMA licenses, while other common ones, e.g. Windows Media and iTunes, can also be supported if respective information is available. The translation manager can be requested to export an MPEG license into any other supported format. The import/export functionality of the DRM-Core provides interoperability with other systems.

Key Store

A particularly important component of the core is the key store. The key store contains the keys which were used to protect content in the system. The core ensures that a content key is given out only when a requested action is allowed by the license. The key store is organised as a table which contains keys and unique content identifiers. The same identifiers are used in the licenses to reference content. Respective technologies are part of the MPEG-21 standard. The key store is implemented as an encrypted file, which is decrypted by the core when a secure environment is established. This is done with the help of the TPM, which seals the key store master key, so that it can only be accessed in a particular system integrity state. The core itself is thus only able to retrieve the master key when the system is secure.

Discussion

Multimedia content is used in a variety of industrial branches. As described above, the health sector is a good example for the reasonable usage of a DRM system. Another application is in the entertainment sector, where video and audio files need protection. In that case, the system provides fairness towards the user as well as to the owner of the content. In the e-learning sector the system can be used as a cheap and standardised solution to protect important multimedia content. The standardisation enables the system to work on different platforms, a fact that is useful in teaching facilities with large heterogeneous networks.

We believe that by using the advantages a trusted computing environment provides, we can develop a successful DRM-System. The important advantages our system will have are:

- Interoperability with other DRM Systems
- Transparency
- Convenience for the user
- Support of legacy software

Our approach differs from other DRM-Systems, because it will be open-source and uses the TPM-Chip to enforce security. Today, many systems are obscure and it is essential for them to keep the encryption methods secret. In contrast to that, open source means that every user can observe exactly what happens with the licenses and the keys. In combination with the TPM-Chip a secure and trustworthy system can be designed, which enforces all applications to work according to their specification. Security is then based on the manufacturer of the TPM-Chip, who ensures and certifies that it is a trustworthy hardware component.

In our project we also would like to involve the Open Source Community. Generally, we expect a negative reaction because our system works basically as a usual DRM System. The Draft version of the GPLv3 gives an impression about the emotional attitude towards DRM. In our point of view the principal problem of DRM is that it is not transparent enough for the user. But this is not a technical problem; it is an effect of the marketing and business models behind the content. These models are so restricted that user interference is often needed.

We hope that participation of the Community in our project will improve such problematic aspects. The project will be available under the GPL, so that the system can even be extended by the open-source community if the need arises. In that way, we want to enable the Linux community to use the advantages of Trusted Computing based DRM for protecting arbitrary data.

Sources

- MPEG: MPEG-21 Multimedia Framework Part 1: Vision, Technologies and Strategy.
  Reference: ISO/IEC TR 21000-1:2004. From ISO/IEC JTC 1.29.17.11.
- MPEG: MPEG-21 Multimedia Framework Part 3: Digital Item Identification.
  Reference: ISO/IEC TR 21000-3:2003. From ISO/IEC JTC 1.29.17.03.
- MPEG: MPEG-21 Multimedia Framework Part 4: Intellectual Property Management and Protection Components.
  Reference: ISO/IEC TR 21000-4. From ISO/IEC JTC 1.29.17.04.
- MPEG: MPEG-21 Multimedia Framework Part 5: Rights Expression Language.
  Reference: ISO/IEC FDIS 21000-5:2004. From ISO/IEC JTC 1/SC 29/WG 11.
- MPEG: MPEG-21 Multimedia Framework Part 6: Rights Data Dictionary.
  Reference: ISO/IEC TR 21000-6:2004. From ISO/IEC JTC 1.29.17.06.
- Open Mobile Alliance (2005): DRM Specification Candidate Version 2.0.
  http://www.openmobilealliance.org/release_program/drm_v2_0.html
- OpenTC-Project Homepage: http://www.opentc.net/
- Trusted Computing Group (2004): TCG Specification Architecture Overview. Trusted Computing Group, Incorporated. Revision 1.2.

About the authors: Dipl.-Ing. *Florian Schreiner* is a research and teaching assistant at the Institute for Data Processing, Technische Universität München. Contact: schreiner@tum.de

Dr.-Ing. *Michael Pramateftakis* is a research and teaching assistant at the Institute for Data Processing, Technische Universität München. His research field is system security and cryptography. Contact: pramateftakis@tum.de

Dipl.-Ing. *Oliver Welter* is a research and teaching assistant at the Institute for Data Processing, Technische Universität München. His research field is public key systems and their application. Contact: welter@tum.de

Status: first posted 01/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=184

iPod's hegemony challenged – new music-enabled smart phones enter the market

By: Gergely Tóth, SEARCH Laboratory, Budapest, Hungary

Abstract: The upcoming version of the Symbian operating system for mobile phones – announced for the Nokia N91 and the Sony Ericsson W950i multi-media phones – introduces Trusted Computing based security features like secure software installation and restricted data storage locations – core requirements for a secure DRM platform. On the other hand, the main novelty of these phones is their 4 GB internal hard disk directly aiming for mass music storage. This step marks the dawn of real music-enabled mobile phones. However isn't it too late to compete with Apple's iPod?

Keywords: news analysis – DRMS, mobile music, portable players, security, Trusted Computing

Introduction

Symbian is the operating system of a wide variety of so called smart mobile phones providing an open development environment for different mobile vendors and mobile operators. As of December 2005, worldwide shipments of Symbian OS phones reached 58.8 million phones (source: Symbian website).

The newest version of the operating system, version 9.1 is just about to appear in commercially available mobile phones. Both Nokia and Sony Ericsson have announced phones based on this version, most notably the Nokia N91 and the Sony Ericsson W950i type. While one of the most important novelties of the new OS is a Trusted Computing based security model (especially suitable for DRM), the main customer-attracting function is to act as an easily usable music player – undoubtedly an attempt to gain a foothold in the Apple iPod-dominated market segment.

In this article first the Trusted Computing based security model of Symbian v9.1 will be introduced, then I will evaluate the possibilities of using v9.1 for DRM, and finally I will look into the chances of the music-enabled phones to become real competitors of the iPod.

Platform security in Symbian OS

The implementation of the Trusted Computing concept in the new Symbian operating system is called Platform Security and its main security functions are the following:

- In the **capability model** so called capabilities (similar to permissions) are assigned to groups of sensitive operations (e.g. network access, PIM access, local connectivity or camera access). Only processes having the corresponding capabilities can carry out the given sensitive operation.

Capabilities are grouped: the most critical (e.g. access to all files of the phone) form the Trusted Computing Base (TCB), which allows full access to all system resources; the Trusted Computing Environment (TCE) comprises capabilities for selected system services and finally all other capabilities are user-visible. Naturally, only a small, highly trusted group of applications will have TCB capabilities, most programs will only have user visible capabilities at most.

- Symbian v9.1 incorporates a **secure software installation mechanism**: only digitally signed applications can be installed. The set of capabilities assigned to the applications is included in the installation package (also protected by the signature) and cannot be altered. The signatures are centrally issued (by Symbian, see SymbianSigned, or by the vendor or operator) only after the developer has been reliably identified and the need for the required capabilities is justified.

  A crucial property of v9.1 is that applications cannot be modified after they have been installed – the kernel (i.e. the system's innermost core) ensures that the location of executable applications is read-only, thus only what has been digitally signed can run on the phone. This means that no third party program can be run on the system with crucial capabilities without prior authorization, thereby mitigating the chance that hackers gain access to the system and also the possibility of virus spreading can also be effectively limited.

- Finally, the OS enforces **separation of the applications and processes**. During run-time applications cannot access each other's memory area except for carefully guarded inter-process communication, whereas for persistent storage each application may create a private directory to which only that application has access. This technique is called data caging, so storing sensitive data in private directories applications can protect their assets from other applications and therefore even against the user himself.

With these new features Symbian took a large step forward providing a secure mobile platform – a risky undertaking considering that the new architecture broke compatibility with the old one, thus previous applications of Symbian v6 and v7 will not run on v9.1. It remains to be seen whether this change was worthwhile, only time will tell the real strength of the architecture since there are currently no devices on the market with Symbian OS v9.1 and thus it has not yet been tested by the community.

DRM based on platform security

Although the aim of Platform Security was not mainly to provide a secure architecture for Digital Rights Management, Symbian v9.1 surely is a starting base for DRM:

- Due to the secure **software installation mechanism** and the **capability model** (as DRM is also guarded by a dedicated capability) only digitally signed and designated applications can access DRM services thus limiting the possibility of unauthorized access. The fact that only tested, signed (and thus back-traceable) applications are allowed to run on a phone is also in favour of DRM.
- On the other hand **data caging** is especially useful for storing secret DRM information (e.g. keys or usage count for limited access assets), since only the dedicated DRM application has access to these pieces of information and thus the secrets can be effectively hidden from unauthorized parties.

These special functions make Symbian v9.1 a safe choice to implement a DRM system.

Music players based on Symbian v9.1

In 2005 Nokia announced the N91 music-enabled mobile phone with 4 GB internal storage for multimedia files. Sony Ericsson soon followed with the W950i, which has similarly 4 GB of space for multimedia. Although neither of them is available on the market yet, both are planned to have Symbian v9.1 as the operating system. While it is yet unsure what DRM solutions W950i will support, Nokia has already announced full

OMA DRM 2 and Windows Media DRM 10 support for N91.

Up till now mobile phones on their own did not have enough capacity to store a reasonable amount of music files internally, and only high-end models were outfitted with some sort of memory card slots to be able to play music files from removable storage. This was clearly inferior to Apple's various iPod versions where the smallest version has 1 GB internal storage capacity (and larger ones going up to 60 GB). With this first step of 4 GB internal drives the mobile vendors demonstrate their decision to enter the market of portable music players. What can be the advantages of such devices against the market-dominant iPods?

- First of all these devices are not just music players, they are fully featured **smart phones** with a wide variety of functions ranging from office applications, PIM services to naturally all kinds of connectivity (GSM, GRPS, 3G, Bluetooth and sometimes even W-LAN etc.).
- Secondly, Nokia has already demonstrated the will to support multiple DRM formats (namely OMA DRM2 and Windows Media DRM 10). This will not only attract content providers but also customers as music from different platforms can be accessed and shared. Many surveys clearly showed that **interoperability** is a key advantage in case of DRM solutions.
- Finally, Symbian-based platforms have a **reputation of being secure** – whereas installing a custom OS onto iPod has a lively community (see the iPodLinux homepage) and the Fairplay DRM system has already been circumvented (Orlowski, 2004), cracking or re-flashing a Symbian-based phone has not yet been demonstrated in public.

All these advantages and the ease of usage will compete with the dominance of iPod and iTunes.

Bottom line

Apple's dominance with the iPod music player on the market is unquestionable; however the competition is slowly starting to react. The newest potential rivals arrive in the form of smart phones with 4 GB of internal storage for music files. The device from both Nokia and Sony Ericsson are based on the upcoming operating system of Symbian with enhanced security functions based on Trusted Computing. The applicability of such phones for DRM-based solutions is obvious, thus support from content providers can be anticipated, and their rich feature set may provide them with an advantage over the iPods. The question is whether the market will also appreciate these devices and how the different DRM solutions will be affected – could it be that this new competition will enforce their interoperability?

Sources

- Symbian OS – the mobile operating system, London, UK: http://www.symbian.com
- Nokia Nseries N91 – http://www.nokia.com/n91
- Sony Ericsson W950i – http://www.sonyericsson.com
- SymbianSigned – http://www.symbiansigned.com
- Apple iPod – http://www.apple.com/ipod
- iPodLinux – http://www.ipodlinux.org
- Orlowski, A (2004).: New workaround for Apple DRM, The Register, April 6, 2004; http://www.theregister.co.uk/

About the author: *Gergely Tóth* is a researcher at SEARCH Laboratory, Budapest, Hungary. Besides Digital Rights Management his core interests include security and privacy. Please visit http://www.planeforge.com/home/tgm.

Status: first posted 02/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=185

Legal risk assessment of Trusted Computing. A review

By: Arnd Weber, ITAS, Karlsruhe, and Dirk A. Weber, IT-Consultant, Bad Homburg, Germany

Abstract: In this article, potential legal issues of Trusted Computing are presented as discussed by legal scholar Stefan Bechtold. This review not only summarizes the main risks identified by Bechtold, but tries to add to the debate.

Keywords: Review – copyright, DRMS, privacy, regulation, secure operating system, Trusted Computing.

Introduction

The main article reviewed here is “Trusted Computing. Rechtliche Probleme einer entstehenden Technologie” (“Legal problems of an emerging technology“; Bechtold 2005b). This article is based on a presentation given at the U.S. Stanford University in March 2005, the slides and talk of which are available in English (2005a). Bechtold published a slightly updated version of his article, again in German (2005c). There is also a further article on TC taken into account for this review (2004b) referring to a somewhat earlier stage of TC-developments.

The reasons for this review is that Bechtold provides quite a dense and comprehensive assessment of potential legal problems associated with Trusted Computing, in particular in the area of DRM. Areas in which legal problems might emerge are identified, and recommendations are given to policy makers and those building “Trusted Computing” systems.

Background of Trusted Computing

“Trusted Computing” is a notion used by the “Trusted Computing Group” (TCG), which emerged from the former TCPA, the Trusted Computing Platform Alliance, which was founded in 1999. At that time, there had been discussion whether computers should have identifiers (cf. the discussion about the Personal Serial Number in the Intel Pentium-III processor; STOA 1999). As the TCPA suggested to have a unique identifier in each “Trusted Platform Module”, observers were worried that it might be aimed at tracing PC users in general, as opposed to using the identifier only for purposes such as identifying parties in electronic commerce. When Microsoft considered using the Trusted Computing approach for basing a DRM-system, “TC” obtained a somewhat negative image in many popular media, blogs, etc. Today, the TCG is led by AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft and Sun.

Key security concepts in the TCPA specifications were based on work by Arbaugh et al. (1997). The process the authors designed is “constructing a chain of integrity checks, beginning at power-on and continuing until the final transfer of control from the bootstrap components to the operating system itself. The integrity checks compare a computed cryptographic hash value with a stored digital signature associated with each component” (Arbaugh et al. 1997). In TCPA/TCG implementations, the chain of trust starts accordingly with the “Trusted Platform Module” (TPM), basically a smartcard chip. Today, TPMs in PCs are mainly used for secure log-in, protection of cryptographic keys, and file encryption support. Checking the whole chain of trust, e.g., operating system, drivers and applications, has not yet been implemented.

The subject of Bechtold's analysis

Bechtold reviews the actual specifications written by the Trusted Computing Group, as well as operating system developments, such as Microsoft’s “Next Generation Secure Computing Base” (NGSCB; variants of new Microsoft operating systems will increasingly support applications based on TC concepts). In addition, he takes into account recent hardware developments, in particular the new processor architectures from Intel and AMD that offer support for “curtained memory “ and “virtualization”. Curtained memory allows for strong isolation between different execution environments, while virtualization allows several different, even unmodified operating systems to run in parallel. Next to a legacy OS, another one could run, e.g. a custom-made one for a content application. With the help of the TPM, it can be determined what is actually running.

The following potential characteristics of Trusted Computing are highlighted:

1. Remote attestation: Comparison of the actual state of a platform with its expected state (validation).
2. System compartmentalisation: With the new processor architecture, e.g., a Trojan horse would not longer be able to read data from a banking application, as these would run in different compartments.
3. Sealed storage: Data are encrypted and can only be read if the system is in a certain state (for making sure that, e.g., no software is running which is designed to "rip" content).
4. Secure input/output: Keyboard, mouse and display are protected against manipulation.

From this list, we see that in frequent cases envisaged by the proponents of TC, "trusted" means that a third party can be enabled to check whether a remote computer can be trusted. Whether a "trusted computer" is trusted by the user, can deserve to be called "trustworthy", etc. is a different matter. As Pearson, editor of an early book on TC, put it when describing the TPM: "This security hardware contains those security functions that *must* be trusted." (2003, p. 5; emphasis in the original). Whether it is trusted in social and economic terms, is a different matter, however.

Risk analysis

Generally speaking Bechtold argues that there are possibly many risks arising, but that they could be dealt with by skilful design of TC-architectures and the institutional arrangements around them. We pick up here the most important points in slightly more detail:

- Remote attestation could be used to hinder inter-operability. It could be ensured that only a certain piece of software, e.g. a Microsoft browser, can be used for getting certain services. He discusses technical remedies such as communicating only properties of a program, or attesting only the correctness of small part of the computer, e.g., a compartment, as well as legal remedies to prevent abuse of market power.
- The role of third parties providing basic keys and metrics for using TC is an issue. For instance, the integrity of software might be checked by comparing its hash value against the one it is supposed to have. Currently, the TCG specifications do not define who these entities will be. It could be, for instance, a large corporation doing it in its own interest. However, central authorities could emerge with a significant market power. Therefore it is of potential relevance that there will be several competing companies or organisations certifying such data.
- Given the market power of dominant players such as Microsoft, the article argues, users might be forced to use TC. For instance, banks might require the use of TC. The author demands to take such dominance, or market failures, into account.
- "Sealed storage" might be used to ensure that certain data formats need to be used. Trusted Computing "can be used to 'seal' data to a particular software state on a platform. In a DRM system, this feature could be used by content providers to make sure that their content may only be accessed by consumers if their devices are in a secure state. However, it could also be used to seal data to a particular operating system, platform configuration, or software application. Software companies could develop proprietary file formats for their applications that can read this file format and thereby interoperate. As the costs of converting files would be significantly increased, this could deter customers from switching to competing applications, operating systems and even hardware platforms in the first place.

Content providers could make sure that their content is only accessible with a particular proprietary player. In general, sealed storage could hamper competition in the hardware, operating system and the software applications markets. Trusted computing could prove a powerful tool to create customer lock-in and artificially increase switching costs." (2004b, p. 88f). Competition law would be a way to deal with the issue.

- TC could be used to design a highly secure DRM system which would be difficult to circumvent. TC could be used to prevent the computer user from copying content from one system to another, as more easily possible with other DRM systems. He concludes that "DRM systems which are based on trusted computing architectures may come into conflict with copyright law... If copyright limitations allow a consumer to copy content to another device without the rights holder's permission, the trusted platform could nevertheless prevent such copying as the sealed content could not be decrypted on the other device." (2004b, p. 95)
- The use of keys could lead to a loss of privacy. Not only could a company verify whether one of its PCs is accessing its network, other companies could also identify platforms and concatenate keys and user identities. Bechtold reviews the merits of "Privacy Certification Authorities" providing pseudonyms and so-called "Direct Anonymous Attestation" which could be used to provide a higher level of anonymity (cf. TCG 2003).

The article also addresses other issues, such as using related patents to limit competition.

Discussion

The reader gets the impression that Bechtold intends to warn of potential negative effects. In contrast to earlier such warnings, e.g. Ross Anderson's, he separates issues of TC (according to the TCG specifications), Microsoft's plans, and DRM very clearly (cf. Safford 2002). In this sense, his work is a very useful early warning.

Summarising one can say that there are three major risks:

1. Dominance of players. This could result in high prices, and in particular the use of open source software could be hindered if certificates were made available only with a delay or at excessive cost.
2. Loss of capabilities to exploit copyright limitations.
3. Loss of privacy.

These could be addressed by the following remedies:

1. Remote attestation could be requested from only a small part of a computer, e.g. a compartment.
2. Competing operating systems and competing institutions providing keys and hash values would be necessary for consumers to have a choice. Thus, a possible abuse of market power would be hindered. With enough competition, applications not using TC would also remain available.
3. Control of abuse of market power through the policy maker.
4. Privacy Certification Authorities and Direct Anonymous Attestation could be deployed to provide more privacy.

With respect to the design of DRM systems Bechtold believes in "value centered design" enabling DRM-implementations preserving copyright limitations, such as private copies (cf. 2004a).

The reviewers would like to bring up a few issues for discussion:

First, Bechtold has a fairly short list of positive effects, essentially stating that digital signatures could be implemented more securely. Other potential effects of TC, such as increased security against theft of data, e.g. from stolen laptop computers, are underemphasised. Also the potential of secure computers to make fighting malicious code less important is underemphasised. But elaborating on such benefits was apparently not within the scope of his article.

Second, Bechtold seems to have the impression that all the hard- and software which is envisaged to be built based on the TCG-principles will work properly. This may not be the case, however. It is by no means guaranteed that it will be possible to implement all the functions in an error-free way. He writes, e.g., that existing PC-architectures need only be "marginally modified" (2005b, p. 394), or that "Trusted Computing will offer a much higher level of security" (p. 404) or that "it is impossible for insecure software, viruses and other dangerous programs to hide their existence on a Trusted Computing-platform" (p. 399). This will only be the case if TC is implemented perfectly. In particular, it seems doubtful whether a permanent attestation is feasible. If attestation is not permanent, but e.g. takes place only during the system's boot process, malicious code, cracking software, etc., might run even in a verified compartment. Regarding DRM, there is also the challenge to build PCs which make it difficult to eavesdrop data somewhere. Applying the BORA principle, cracked content could run undetected in a future, separate compartment. Protections such as watermarking might perhaps remain, though, and the process might be illegal, which would reduce such abuse.

Third, there is the interesting issue whether Microsoft will aim at blocking virtualisation regarding non-Microsoft operating systems and compartments. New Microsoft operating systems could ensure, with the help of the TPM, that they only run if no other compartments with different operating systems are running. This would hinder competition.

Bottom line

One could regard Bechtold's worries as an example of German thoroughness and of scepticism with regard to new technologies. It seems, however, his work is right in time, as there is a good possibility that during the next few years hundreds of millions of TPMs will be in PCs. Therefore it is important to monitor whether Trusted Computing will lead to secure systems, or to lock-in. Regarding DRM, Bechtold warns that TC might prevent users from exploiting rights provided by the copyright law, so this issue will also warrant continued monitoring.

Sources

- Anderson, Ross (2005): Trusted Computing. Frequently Asked Questions. Access 16.12.2005. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Arbaugh, William; Farber, David; Smith, Jonathan (1997): A secure and reliable bootstrap architecture. In: Proceedings of the 1997 IEEE Symposium on Security and Privacy, pp. 65-71; http://www.cis.upenn.edu/~waa/aegis.ps
- Bechtold, Stefan (homepage): http://www.bechtold.name/
- Bechtold, Stefan (2004a): Value-centered design of Digital Rights Management. INDICARE Monitor, Vol. 1, Number 4, September 2004; http://www.indicare.org/tiki-read_article.php?articleId=39
- Bechtold, Stefan (2004b): Trusted Computing Initiatives – Protecting virtual Troy or creating a Trojan horse? In: Koenig, Christian; Neumann, Andreas, Katzschmann, Tobias: Trusted Computing. Technik, Recht und gesellschaftspolitische Systemumgebungen. Heidelberg 2004 pp. 77-99
- Bechtold, Stefan (2005a): Trusted Computing: Whom do we trust? Presentation given at Stanford Law School, March 2005. Slides and talk available at: http://cyberlaw.stanford.edu/events/archives/stefan_bechtold_2005.shtml
- Bechtold, Stefan (2005b): Trusted Computing. Rechtliche Probleme einer entstehenden Technologie. In: Computer und Recht 6/2005, 393-404 (2005b)
- Bechtold, Stefan (2005c): Update of Bechtold 2005b; http://cyberlaw.stanford.edu/blogs/bechtold/tcblog.shtml
- Intel (2003): LaGrande Technology Architectural Overview. http://download.intel.com/technology/security/downloads/LT_Arch_Overview.pdf
- Pearson, Siani (ed.) (2003): Trusted Computing Platforms. TCPA technology in context. Upper Saddle River 2003
- Safford, David (2002): Clarifying Misinformation on TCPA. IBM Research 2002; http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf
- STOA (Scientific and Technological Options Assessment) Panel, European Parliament: Development of Surveillance Technology and Risk of Abuse of Economic Information. Luxembourg, April 1999; http://www.cryptome.org/stoa-r3-5.htm

► Trusted Computing Group (2003): TPM v1.2 Specification Changes. October 2003. https://www.trustedcomputinggroup.org/

About the authors: *Arnd Weber*, researcher at ITAS, is currently participating in the OpenTC project (http://www.opentc.net). Recent research addressed success factors of the Japanese mobile data (and music) market. He has also done work on "secure wallets" in the framework of EU-projects CAFE and SEMPER. *Dirk A. Weber* has experience with managing corporate networks as a Microsoft Certified Systems Engineer and as a Certified Novell Engineer. Contact: arnd.weber@itas.fzk.de and dirk.weber@compuserve.com.

Status: first posted 02/03/06; licensed under Creative Commons; included in the INDICARE Monitor of February 2006

URL: http://www.indicare.org/tiki-read_article.php?articleId=186

Masthead

The INDICARE Monitor is an electronic periodical of the EU-funded project INDICARE being published every last Friday of a month. Articles having passed an internal review process are immediately posted at the INDICARE homepage for public debate. Authors are encouraged to revise their articles in the light of previous discussion before publication in the monthly issue.

- You can use the *RSS-feed* to get articles as soon as they are posted.
- You can *subscribe* to the INDICARE Monitor, and receive an *e-mail notification* containing the contents page (title, author, abstract, and URLs) and a link to the pdf-version (this service replaces the bi-weekly INDICARE newsletter). Just type in your e-mail address at the INDICARE Website and Go!, or send an empty e-mail to: indicare-monitor-subscribe@indicare.org
- The *INDICARE Monitor Archive* offering all issues in HTM and PDF is available at http://www.indicare.org/tiki-page.php?pageName=IndicareMonitor
- The *INDICARE Homepage*: http://www.indicare.org/

Editorial Team: The Editorial Team currently consists of Knud Böhle, Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe, Germany (Editor); Michael Rader, also from ITAS (Copy-Editor); Nicole Dufft, Berlecon Research GmbH, Berlin, Germany (Co-Editor business); Natali Helberger, Institute for Information Law, Amsterdam, The Netherlands (Co-Editor legal), and Kristóf Kerényi, SEARCH Laboratory of Budapest University of Technology and Economics (Co-Editor technology).

Editorial policy: The INDICARE Monitor is an English language periodical publishing original works. The editorial policy attempts to be balanced, unbiased, neutral, and non-partisan, not excluding however provocative, pointing and sometimes even lopsiding contributions. Articles are written by INDICARE staff and external experts. The style is intended to be analytical, concise, compact, and written in a language comprehensible for non-experts. The expected length of an article is between 5000 and 10.000 characters. The INDICARE Monitor is available for free.

Disclaimer: The views and opinions expressed in the articles of INDICARE Monitor do not necessarily reflect those of the European Commission and the INDICARE consortium or partners thereof. All articles are regarded as personal statements of the authors and do not necessarily reflect those of the organisation they work for.

Acknowledgment: The INDICARE Monitor is an activity of the INDICARE project, which is financially supported as an Accompanying Measure under the eContent Programme of Directorate General Information Society of the European Commission (Reference: EDC - 53042 INDICARE /28609).

Contact
Knud Böhle (Editor)
Institute for Technology Assessment and Systems Analysis (ITAS)
Phone: +49 (0)7247/82-2989 (-2501)
Fax : +49 (0)7247/82-4806
E-Mail: knud.boehle@itas.fzk.de