INDICARE Monitor

About Consumer and User Issues of Digital Rights Management Solutions

www.indicare.org **ISSN 1614-287X**

INDICARE Monitor Vol. 2, No 10, December 2005

Content

Editorial of INDICARE Monitor Vol. 2, No 10, 23 December 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: In the editorial we announce the report of the 3rd INDICARE Workshop about "Fair DRM Use", hint to the call for contributions to the 5th INDICARE Workshop about "Human Factors of DRM" (Budapest 19/01/06), and express our wish for more INDICARE Monitor articles from Northern, Southern, and Eastern Europe. The five articles published in the December issue cover BEUC's reasons for its Campaign on Consumers' Digital Rights, a review of a study commissioned by BEUC testing the interoperability between online music stores and portable players, an introduction to DVB-CPCM, the content protection and copy management system proposed by DVB for digital broadcasting, and finally a conference report about DRMTICS 2005 and a second about Axmedis 2005.

Keywords: editorial – INDICARE

INDICARE news

The *3rd INDICARE Workshop* about "Fair DRM Use" was organized by the Institute for Information Law (IViR) and took place in Amsterdam, 28 May 2005. Meanwhile *Mara Rossini* and *Natali Helberger*, both from IViR, have produced a concise and well written workshop report (Rossini and Helberger 2005), which is available online. It summarizes and synthesises presentations and debates. While the first part of this 18-pager deals with consumer expectations and consumers' legitimate interests, the second part is about political and regulatory options for consumer protection.

The *5th INDICARE Workshop* about "Human Factors of DRM", scheduled for the 19th of January 2006 in Budapest is organized by INDICARE partner SEARCH. The aim of the workshop is to put the consumer and his needs in focus analysing DRM-protected offerings and devices from a human factors point of view. Special attention will be given to the access problems of potential users living in less developed countries and groups with special needs like disabled persons. Don't hesitate to contact the organisers if you would like to present at the workshop or to participate. To learn more about the workshop, please have a look at the "Call for presentation" at our website (cf. sources).

Towards the end of the year, when wishes are more likely to come true, I would like to express our INDICARE Monitor wish for the next year: users and consumers of DRM systems from Northern, Eastern and Southern Europe contribute to the INDICARE Monitor! It is meant to be a truly European online journal covering experiences and opinions from all over Europe. Help us to better achieve this goal!

About this issue

BEUC's criticism of European policy

BEUC, the European Consumers' Organisation, and other consumer organizations have been denouncing for a long time shrinking consumer rights in the digital environment - the Sony BMG scandal being just the tip of an iceberg. What bothers BEUC most as a European high-level interest group is apparently the feeling that their arguments remain - so far - unheard by European policy makers. Consequently they started a Campaign on Consumers' Digital Rights. The article by *Cornelia Kutterer* is however much more than a description of this campaign. It is but a serious attempt to investigate cases of ongoing policy making showing how the interests of consumers are ignored or weakened in these processes. An essential weakness of European policy is seen in the conflation of commercial infringement of copyright (piracy) and non-commercial copyright infringement, ending up with a notion of piracy as first of all non commercial infringement.

Intertek's interoperability study

Kristof Kerenyi, SEARCH, contributes a knowledgeable review of an interoperability study performed by *Intertek Research and Performance Testing* and commissioned by

BEUC. UK-based music services and widely available digital music players were compared and tested with a focus on interoperability of file formats and DRM formats. The main results are presented in the review. The review highlights the value of the study as easy to read "educational material" for the public making aware of DRM systems' limitations today - including hints how to achieve interoperability nonetheless.

DVB's Content Protection & Copy Management specifications

Chris Hibbert, Vice President Media Technologies & Standards with Walt Disney Television International, gives an excellent introduction to the Content Protection & Copy Management (DVB-CPCM) system developed by the Digital Video Broadcasting Project and published in November 2005. More precisely the first three elements of this specification have been published. DVB, established in 1993, is today a consortium of c. 300 companies from more than 35 countries committed to develop pan-European open standards for digital broadcasting.

The article does not go into technical details, but gives a high-level overview of the main features of the DVB-CPCM specifications and the work still ahead. Apart from the clear presentation of a rather complicated subject, I do appreciate that Hibbert also explains the context of this standardisation effort: the changing scope of DVB activities, the motivations behind DVB-CPCM, and even lines of conflict.

Conference reports

Rei Safavi-Naini, *Wanqing Li* and *Nicholas Sheppard* all involved in the organisation of DRMTICS 2005 provide you with a comprehensive conference report. DRMTICS, Digital Rights Management: Technology, Issues, Challenges and Systems, took place in Sydney from October 31 to November 2. The interdisciplinary character of the conference is worth highlighting. As the full proceedings of the conference will be available in Springer's Lecture Notes in Computer Science later in 2006 this report is a good opportunity to get first hand impressions and an overview of the event.

Gergely Tóth, SEARCH, reports about Axmedis 2005, the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution taking place in Florence, November 30 to December 2. Although Axmedis is mainly a large European R&D project (FP6 Integrated Project) addressing cross-media production and distribution, the conference was interdisciplinary in nature. This was achieved by organising additional panels and sessions devoted to user and consumer aspects of digital media and DRM. For instance a panel was organized on collecting societies, the EUAIN, the European Accessible Information Network, organized a panel, and in particular the "digital goods workshop" (the third in a series), which addressed user and consumer aspects in digital goods markets, was incorporated in the conference framework. As the conferences proceeded in parallel sessions, the present conference report can of course not cover all. The good quality of the conference makes me therefore recommend the two printed volumes of the proceedings, which are already available.

As you will have noticed, this INDICARE Monitor is not published last Friday of a month as usual, but the last but one due to Christmas time. We wish you the very best for the holidays to come and the next year

the INDICARE team

Sources

- Rossini, Mara and Helberger, Natali (2005): Fair DRM Use. Report on the 3rd INDICARE Workshop Held on 28 May 2005 in Amsterdam; available at http://www.indicare.org/tiki-download_file.php?fileId=146
- 5th INDICARE Workshop on the Human Factors of DRM: CALL FOR PRESENTATION: http://www.indicare.org/tiki-page.php?pageName=WorkshopFiveCall

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 23/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=164

Some of the reasons for BEUC's Campaign on Consumers' Digital Rights

By: Cornelia Kutterer, BEUC, and Brussels, Belgium

Abstract: This article explains the reasoning behind BEUC's "Campaign on Consumers Digital Rights". Current international IPR policy, in particular that of the European Union is perceived as a danger to established rights of consumers. This opinion is put forward supported by a series of arguments and examples.

Keywords: opinion - consumer protection, data protection, digital TV, DRMS, EU policy, piracy, private copy - EU

Introduction

The ease of digital copies has challenged traditional business models by lowering the cost and effort of reproduction and distribution. Different business models for content delivery compete in a fast developing technological environment. As a result, values such as the protection of Intellectual Property Rights (IPRs) on the one hand and the protection of the private sphere and consumers on the other seem to be more and more at odds.

Even voices from industry confirm the threat. In the words of *Gary Shapiro*, president and chief executive of the Consumer Electronics Association (CEA): "In the rush to crack down on pirates, we risk eliminating a critical consumer right – the right to use copyrighted material, without the permission of the copyright owner" (quoted in Taylor and van Duyn 2005).

But generally industry tends to ignore the interests of consumers. A notorious example is Sony BMG's director for digital business, *Thomas Hesse*, who stated - when debate about the Sony BMG debacle over its intrusive DRM system heated up: "Most people, I think, don't even know what a rootkit is, so why should they care about it?"(quoted in Orlowski 2005; cf. Bohn 2005 for more debate on the Sony BMG debacle; cf. also Doctorow 2005a). It may possibly be true that many consumers are not aware of DRM (cf. the results of the INDICARE survey, Dufft et al. 2005), let alone the effects it may have on their private lives. But does that mean that they shouldn't care about it? Can we watch the societal shift from young people taping at home in a private sphere to a generation surveyed and criminalized?

Facing these threats, it seems astonishing to the naïve reader that *Charlie McCreevy*, Commissioner for Internal Market and Services, stated in a recent speech before the BSA (European-American Business Council/Business Software Alliance) that "the pure technology issues such as the robustness of the technology, the acceptance by consumers can be left to the market" (McCreevy 2005). Another example of the weak standing of consumer interests in public policy is the "EU-US Initiative to Enhance Transatlantic Economic Integration and Growth". While the Commission has acknowledged in a draft implementation paper of this EU-US Initiative that there is – in respect to DRM and technical protection measures - a need of "taking due account of public policy interests, such as the promotion of fair competition and consumer rights, with a view to identify best practices", in the final version this sentence was deleted - due to US pressure (cf. EU-US 2005).

Consumer organizations have been denouncing for a long time shrinking consumer rights

in the digital environment (cf. e.g. BEUC 2004) but remained so far unheard by European policy makers. It is against this background that on 10 November BEUC, the European Consumers' Organisation, launched a *Campaign on Consumers Digital Rights* supported by *Zusana Roithova,* Member of the European Parliament. The Sony BMG story merely underlined the necessity for this campaign and revealed that many of the issues addressed are not only "potential but unlikely risks" - instead - these risks have materialized. In the following we will point out some more European and international developments threatening consumers' rights by fostering technical protection measures and expanding criminal law. They all demonstrate the need for our campaign.

Blurring the boundaries between commercial and non-commercial copyright infringement

The entertainment industry has successfully watered down specific terms or extended their scope in commonly used language – such as piracy. What is piracy? It is an imprecise term for copyright infringement – in the first place – because it disregards the necessity to differentiate between non-commercial and commercial copyright infringement. While some "pirated content" is simply infringing (you upload a copy-protected music file on a P2P net without permission), other is commercially infringing (somebody sells an illegal copy). The impact of each is different. Conflating them under the "piracy" banner is nonsensical. By the way, conflating non-commercial infringement of copyright under theft is nonsensical as well.

In the 90s, the Commission was willing to distinguish commercial infringement of copyright (=piracy) from non-commercial copyright infringement:

> "Piracy … embraces the unauthorized reproduction of works protected by copyright or allied rights for commercial purposes as well as all subsequent commercial dealing in such reproductions. *The commercial purpose* and frequently the scale on which the activity is carried out are characteristic features which distinguish the practice from other forms of unauthorized reproduction or use such as home copying. Piracy in this sense includes bootlegging, that is, the unauthorized recording of performances and the subsequent marketing of copies of the recording. It is frequently associated with counterfeiting, that is, unauthorized use of a legitimate product commercial presentation, in particular, its trade mark or some other protected indication" (EC 1988).

Today, it appears that the Commission no longer distinguishes these two different types of infringement. But blurring these boundaries leads to excessive reactions that may have deep, irreversible and adverse effects on our society, technological development and the private sphere.

In a highly controversial and often hostile debate about the scope of IP protection, recent developments in the political debate tend to be excessive, disproportional, lopsided and do not take into account the existence of many discussions on how to improve creativity, access to knowledge and the legal use of technology. Instead, the law of unintended consequences is being provoked. Some examples:

Criminalization of consumers

In a recent proposal adopted by the Commission in July 2005, the Commission aims at introducing and aligning national criminal law provisions against infringements of IPRs. Under the proposal, infringements of any intellectual property rights are treated as criminal offences if undertaken intentionally and on a commercial scale. Similarly, attempting, aiding and inciting such infringements are considered criminal acts.

The problem is that the definition of "commercial scale" is not set out, and does not explicitly require financial benefits, profit or a commercial motive for activities to be identified as taking place on a "commercial scale". This may straightforwardly lead to private non-commercial (but infringing) uses being criminalised as of potentially commercial scale (the issue – rejected during the 2004 Enforcement Directive debate – is thus back

on the agenda). The inclusion in criminal behaviour of activities collected together under "aiding or abetting and inciting such infringements" is imprecise and far too inclusive of activities that are entirely legal. Thus, it is possible that an email noting the existence of a piece of peer-to-peer software might be regarded as an incitement to infringe intellectual property rights.

Data retention

At the time of writing, the European Parliament is discussing and adopting a controversial compromise proposal to revise Article 15 of EC Directive 2002/58 that will introduce extensive common rules on data retention (On 14 December, the European Parliament approved at first reading (by 387 votes to 204 and 30 abstentions) the proposal for a directive on telecommunications data retention in the fight against terrorism and organised crime) despite the fact that the European Data Protection Supervisor and the Article 29 Working Party of European Privacy Commissioners have repeatedly stated that the case for retention has not been made and that the scope of that proposal is not proportionate (ARTICLE 29 Data Protection Working Party 2005): The European Data Protection Supervisor has also stated in his opinion, the mere existence of data might lead to increased demands for access and use by industry, law enforcement authorities, and intelligence services.

In the first place, data retention was considered necessary to combat terrorism. The adopted compromise foresees access to this data to combat all serious crimes (a term to be specified by the Member States). The CMBA, Creative and Media Business Alliance, however, lobbied strongly to include all crimes:

> "The scope of the proposal should include all criminal offences. The Directive, as proposed, is limited to the prevention, investigation, detection and prosecution of serious criminal offences such as terrorism and organized crime (Article 1.1). The position of the CMBA is that the scope of the proposal should be extended to all criminal offences. Limiting the proposal to serious offences would hamper the effectiveness of the Directive and the enforcement activities for other forms of criminal offences. Once an illegal activity is considered as a crime in a Member State, the enforcement authorities should have adequate means to prosecute it" (CBMA position on data retention of 22 November 2005).

CMBA would like to use a piece of legislation intended to fight terrorism in order to get hold of P2P-users that infringe copyright (cf. Cronin 2005). Obviously, non-commercial infringement of copyright must be made a crime in the first place.

Internet Services Providers' control of data

Other initiatives also aim at getting hold of the same data. A group of entertainment industry and Internet Service Providers is discussing with the European Commission – in a so-called "Sherpa group" – how best to cooperate to fight piracy (here it seems, the term piracy is used ***only*** for non commercials infringements).

The group is seeking to develop a charter on best practices in order to fight unauthorized file-sharing. The envisioned system would entail a graduated response system ultimately shutting down Internet connections of customers who engage in unauthorized file-sharing. The CMBA issued a statement on the charter on 2 November: "At its core, it should consist of a couple of escalating notices to infringers, culminating in termination, or at least suspension, of subscriptions for recidivists" (CMBA position paper on a EUropean Charter for on-line content of 2 November 2005). A similar procedure in France involved automatic systems to detect copyright infringement on peer to peer networks, and to force internet service providers to translate a given IP-address into an e-mail address and forward a 'pedagogical' e-mail message from the societies to their customer before commencing civil or criminal actions. But the French Data Protection authority CNIL strongly rejected this approach as being disproportional (cf CNIL 2005).

Using ISP's and their contracts as enforcement vehicles raises a number of issues not least privacy but the CBMA statements on

privacy wipes away these concerns: “It has become fashionable for some to claim data privacy constraints to plead against effective actions to tackle infringing activities by individuals. ….. Data protection should not be an impediment to the reasonable retention, preservation and access to evidence for legitimate purposes. It is essential to ensure that infringing activities are not protected by anonymity” (ibid.) The group further tackles liability provisions in the E-commerce directive: “Such a step could serve as one indicator to justify benefiting from the safe harbor provisions of the Electronic Commerce Directive that limit the liability of certain intermediaries under certain conditions” (ibid). This coincides with the Commission initiative to set up an expert group (comprising member states) to discuss the development of the e-commerce directive, in particular regarding ISP liability provisions (a Commission study on this topic is foreseen, see http://europa.eu.int/comm/internal_market/e-commerce/index_en.htm). But take down notices have proven to have little effect, easy to abuse and to come with chilling effects (cf. Urban and Quilter 2005).

Traceability – DRM requirement

NAVSHP

Other initiatives tackle the traceability of data. On September 13, 2005, the "Networked Audiovisual Systems and Home Platforms" group (mainly comprising interested companies) released a paper called "NAVSHP (FP6) DRM Requirements Report (NAVSHP 2005). This is a set of technical and commercial requirements for developing DRM. The purpose of the document was to promote common understanding within the NAVSHP, which in their research work has to tackle the DRM issue, to allow discussion and mutual help on this very complex issue. While the Commission has made explicit that it will not be bound in any way by the output of this activity and that there was no direct discussion on policy, possible legal requirements, etc. – it has also acknowledged the document's deficiencies in these areas.

The DRM specifications require for example: “There is a need to give the DRM system the ability to later prove consumer selections or actions that need to be monitored, in front of a 3rd party. This information can only be disclosed to appropriate authorized systems, in specific and clearly announced cases.” Other requirements also treat users as infringers. It has never been questioned whether DRM should include traceability requirements at all. (for criticism cf. Doctorow 2005b).

DVB

Similar attempts to describe DRM specifications are made by an industry group called the Digital Video Broadcasting Project (DVB). This is an industry-led consortium (with no consumer participation) of over 260 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others in over 35 countries committed to designing global standards for the global delivery of digital television and data services. Its sub groups, CM-CP and TM-CPT, are working to develop the Content Protection and Copy Management (DVB-CPCM) system for managing distribution, copying and redistribution of television content (cf. in this INDICARE Monitor the article by Hibbert 2005), akin to the US “Broadcast Flag” which has been successfully stopped in a recent US court of appeal decision. DVB-compliant solutions will effectively hinder or prevent consumers from recording free over-the-air broadcasting for legitimate time-shifting usages (for criticism see Doctorow 2005c). It will be now submitted to ETSI standardization.

Bottom line

These recent developments and initiatives show that the balance between the rights of the right holders and the rights of consumers is neither achieved nor maintained but instead ever more threatened. Consumers’ organizations have to be very vigilant in the near future. The European Commission has announced a review of a set of directives related to copyright, in particular the reform of copyright levies applied to equipment and media used for private copying and a review of copyright term, above all, term for sound recordings are included in the review. Consumers’ organizations will also need to look at the contractual side and pay high attention

to abusive terms in services. An initiative report on consumer protection in the digital environment by the European Parliament could certainly help to address this issue.

A good sign came recently from The German Federal Supreme Court. It stated that "the necessary balance between the constitutionally protected rights of the right holders to exercise their rights and the constitutionally protected interest in competition, i.e. to be able to evolve freely outside that protected scope, would not be guaranteed anymore if the right holder could claim protection to an extent to which he is not entitled…" (BGH 2005). The court adds that this objective distinction between the scope of IP protection and the freedom of competition must also be balanced in regard to the means of enforcement. We believe that the statement is fundamental and should be reflected in all initiatives at hand.

Sources

- ARTICLE 29 Data Protection Working Party (2005): Opinion 113/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005). Adopted on 21st October 2005; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf
- BEUC 2004: Digital Rights Management (DRM) - BEUC Position paper, X/025/2004, Brussels, 15.9.2004; http://www.beuc.org/Content/Default.asp?PageID=103
- BEUC (European Consumers, Organisation/Bureau Européen des Unions de Consommateurs), Brussels, Belgium http://www.beuc.org – http://www.consumersdigitalrights.org
- BGH (2005): BGH Case GSZ 1/04, July 15 2005.
- Bohn, P. (2005): Intrusive DRM: The cases of Sony BMG, StarForce and Microsoft. INDICARE Monitor, Vol. 2, no 9, November 2005; http://www.indicare.org/tiki-read_article.php?articleId=155CMBA (2005): CMBA statement of 2 November 2005 on 'A EUROPEAN CHARTER FOR ON-LINE CONTENT' (CMBA – A European Charter for on-line Content 2 November 2005) Hibbert, Chris: DVB-CPCM. First steps towards an open standard for a content protection and copy management system from the DVB. INDICARE Monitor, Vol 2, no 10, December 2005; http://www.indicare.org/tiki-read_article.php?articleId=159
- CNIL: Press release of 24 October 2005; http://www.cnil.fr/index.php?id=1881
- Cronin, David (2005): Music moguls want EU terror law to hunt pirates. European Voice of 24 November 2005, http://www.european-voice.com/archive/issue.asp?id=470 (registration required)
- Doctorow, Cory (2005a): Vaudeville offers a music lesson for Sony BMG. Financial Times (FT.com), December 11 2005 (registration required for download)
- Doctorow, Cory (2005b): Critique of "NAVSHP (FP6) DRM Requirements Report. Electronic Frontier Foundation 2005; http://www.eff.org/IP/DRM/NAVSHP/NAVSHP_critique.pdf
- Doctorow, Cory (2005c): Europe's coming broadcast flag: DVB CPCM is a stealth attack on Europeans' digital rights. Electronic Frontier Foundation 2005; http://www.eff.org/IP/DVB/
- Dufft et al. (2005): Digital Music Usage and DRM – Results from an European Consumer Survey, Berlin, May 2005; free download at: http://www.indicare.org/survey
- EC (1988): Commission of the European Communities. COM (88) 172 final . Green Paper on Copyright and the challenge of technology – Copyright issues requiring immediate action. Communication from the Commission. Brussels, 7 June 1988; http://aei.pitt.edu/archive/00001209/01/copyright_and_tech_gp_COM_88_172.pdf
- EU-US (2005): Implementation of the Economic Initiative of the June 2005 EU-US Summit: Joint EU-US Work Programme. Brussels, Washington, November 2005; http://www.europa.eu.int/comm/external_relations/us/economic_relations/joint_eu-us_work_prog.pdf
- McCreevy, Charlie (2005): European Commissioner for Internal Market and Services: Address to the EABC/BSA (European-American Business Council/Business Software Alliance) Conference on Digital Rights' Management. High level Industry Seminar/Global Industry Roundtable on Levies & DRMs. Brussel, 12 October 2005; http://europa.eu.int/comm/commission_barroso/mccreevy/docs/speeches/2005-10-12/euam_en.pdf
- NAVSHP (2005): DRM Requirements Report. Target release version: V1_.0; http://www.ist-avista.org/cg1_files/NAVSHP-DRM-CG_ADT_20051027.pdf

- Orlowski, Andrew (2005): Sony digital boss – rootkit ignorance is bliss. http://www.theregister.co.uk/2005/11/09/sony_drm_who_cares/
- Shapiro, Gary (2005, the CEA president and chief executive, in testimony before a US congressional committee. See in Financial Times 'Music industry asks whether fair use is fair play' by Paul Taylor and Aline van Duyn, 28 November 2005. http://news.ft.com/cms/s/2594a9f8-603a-11da-a3a6-0000779e2340,dwp_uuid=fcd3ba1e-2025-11d8-81c6-0820abe49a01.html
- Urban, Jennifer M. and Quilter, Laura (2005): Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act; (full research paper version of this study will be published in the March, 2006 edition of the Santa Clara Computer and High Technology Law Journal); http://mylaw.usc.edu/documents/512Rep/

About the author: Cornelia Kutterer holds the position of senior legal advisor at BEUC, the European consumer organisation. She is responsible for the legal department focusing on consumer protection law, contract law, passenger rights, intellectual property and information technology laws. She is a qualified German lawyer and holds a master's degree in information technology and communication laws. Contact: CKU@beuc.org

Status: first posted 20/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=162

Music services are incompatible – A research of what we already know

By: Kristof Kerenyi, SEARCH laboratory, Budapest, Hungary

Abstract: An independent institute was "commissioned by BEUC to investigate the limitations that may be present on purchased music downloads from major online suppliers and in particular, how these limitations restrict the consumer's traditional ability to transfer their music between platforms and players." INDICARE analysed the resulting Technical Report, and came to the conclusion, that the right findings were provided in the right form for the public, thus good "educational material" was produced for consumers.

Keywords: review – consumer expectations, consumer protection, consumer research, interoperability, music markets, IT industry - UK

Independent consumer research

The European Consumers' Organization (BEUC) commissioned an independent institute, Intertek Research and Performance Testing, to perform an analysis of some of the UK-based music services and widely available digital music players and find out how interoperable they are, in other words the limitations, and "how these limitations restrict the consumer's traditional ability to transfer their music between platforms and players". This has been an intriguing question for consumers, most of whom have heard about the issue, but in the end they have had to accept the present situation of non-interoperable music download services.

Intertek chose four portable music players:

- an Apple iPod Photo was selected for its compatibility with Apple iTunes Music Store (AAC format files),
- a Creative Zen Micro was selected for its compatibility with MSN Music and Windows Media Player 10 (WMA format files),
- a Rio Carbon was selected for its WMA support (second player with WMA format files chosen because of WMA popularity, and also in order to test a second music store, HMV, using Microsoft's format) and
- a Sony Network Walkman for its compatibility with CONNECT Music Store (ATRAC3 format)

Each player was tested with the corresponding service, and players were also cross-checked to find out what level of interoperability exists, all of this from the layman's point of view.

Technical report

The result of the analysis was a technical report, which is now available for the public on a new web site titled Consumers Digital Rights (cf. sources), created as an information source for a wide range of readers, from politicians through journalists to consumers of DRM-protected content. "On this website we invite you to discover everything you always wanted to know about your consumer rights in the digital environment" – they declare.

Accordingly, the technical report is concise and easy to read, also providing basic information to those not really familiar with digital audio, DRM and related services. The report starts by giving a background to compressed audio, which, as opposed to traditional digital audio like CDs, makes new usages possible: "individual tracks or whole albums can easily be downloaded from the Internet where they can be purchased at lower cost and where new music can be discovered. Also, entire music collections can be copied and stored on a home computer/laptop or portable hard disc based audio file player" (p. 4)

In the following, different compressed audio formats are explained:

- mp3, as the most widespread format does not support DRM, and therefore it is not generally supported by major record companies
- WMA, Microsoft's file format does support DRM. Most music web sites have music available to download in this format, and it is also very popular with the manufacturers of portable players. The reason for the latter is that most modern PCs will already have the Windows Media Player (the player for this format), as the report says, though I have to disagree with this: I think that the main reason is that this is the only widespread technology that is free for everyone to license.
- ATRAC, Sony's file format, also supports DRM. This is said to provide the best sound quality for a given bitrate, but Sony so far has not licensed it to anyone, therefore it is a very proprietary format.
- AAC, the choice of Apple, is employed in the iTunes Music Store. While AAC is an open standard free to implement and use for everyone, Apple coupled it with its proprietary FairPlay DRM system, which makes it inaccessible for any of the few players that manage the compression format itself. (At this point the Technical Report is a bit confusing, saying that "AAC files can only be purchased through the iTunes web site" and suggesting that AAC is a file type supporting DRM. AAC in fact is just the compression method, unlike Microsoft's and Sony's compression-protection formats.)

Actual tests

The report moves on to the actual testing done at the research institute. They created accounts at the mentioned music stores, and bought a couple of songs, trying to play, burn, transfer (copy to a different computer) and transcode (convert to a different format) them. Importing songs to a different media player framework from where they were purchased and loading to portable devices were also main points of investigation.

To cut the long story short, each music store was quite comparable in terms and offerings. Each needed a special media player framework (Apple iTunes, Microsoft Media Player 10, HMV's own software and Sony SonicStage) to handle the music. They could be used for discovering new music, buying, organizing and playing songs and for transferring them to portable devices and finally exporting (burning to CD). Each compression method used about the same compression ratio (around the same file size for the same track). Apple and Sony provided only "permanent purchase" models with unlimited plays for a one-time payment and export options, while the two Microsoft DRM-based systems additionally allowed monthly subscriptions where an unlimited number of songs can be played, but only as long as the

subscription is maintained and after this period the songs become unavailable (the exporting option is in this case disabled).

The report analyses individual terms: number of PCs where purchased songs are playable, number of portable devices they can be transferred to and also the number of CD burns. There were some differences, but to me it seemed that the offerings were all liberal enough to not disturb the ordinary user. Terms were mostly correctly displayed before purchase, but in two cases the testers reported unexpected anomalies: in the MSN Music store "tracks were time restricted to 31/12/2099", which is a bad thing, but personally I do not consider this restriction very limiting to myself, the other was in the HMV store where the DRM system allowed a lot more than was stated before purchase – a nice surprise.

Compatibility

The authors of the report gave this chapter the title "File Compatibility" (page 11), but personally I would have preferred "system compatibility". They tried to import music bought from one system to another system's music library (the collection of music handled by the media player framework). It turned out that the two Microsoft DRM-based systems were (apart from one glitch) compatible with each other, but taking these two as one (since the employed technology was the same) protected music could not be transferred to other systems. This means complete lack of interoperability. Unprotected WMA files can be imported to iTunes and SonicStage, and thus transferred to an iPod, and a Network Walkaman successfully, but AAC and ATRAC files can not be transferred between systems. This is due to DRM-incompatibility rather than file-incompatibility in the case of AAC (since it is an open standard), and due to the incompatibility of both in case of ATRAC (since Sony uses a closed proprietary format) (pages 12, 13 and 14).

What I missed here was the analysis of whether MP3, OGG Vorbis, or other unprotected formats could be imported or exported to and from the respective systems.

Findings

When it comes to the analysis of DRM *systems*, the report becomes rather speculative. What is checked carefully is in particular the contracting terms. Not surprisingly the report discovers that different music stores have different conditions in terms of number of CD burns, portable players, etc.; usage restrictions are not clearly labeled, information on the web sites is not transparent and inconsistent across different music stores and licensing terms are difficult to understand; and by using proprietary formats download web sites can control what one can do with the music and the devices they will play on (cf. Summary, p. 2).

What is more astounding is that "the terms and conditions on these music stores allow the service provider to unilaterally change the terms", and "this would not even break the contract". (cf. Summary, p. 2) On the other hand, technically, it is also possible to change "limitations to a consumers existing collection", which means that in the future there is a possibility for music stores to retrospectively further restrict our purchased music – however, this would be technically challenging and highly unlikely (p. 16).

Yet what made me really wonder was that at the end of the report, in the Appendix, a detailed description is given about how to achieve artificial interoperability between the incompatible systems. More precisely, I was surprised to see this information made publicly available by a high level interest group. Burning the songs to CDs, and then re-ripping them with the target systems' media player frameworks might be a slightly inconvenient, but certainly effective way of lifting the DRM from the protected music (p. 19). And while the report says that this method is "time consuming", my opinion is that it is possible to create tools (and will therefore be such tools) which automatically do this.

Bottom line

The report talks about a media consultant, who said "My only confidence is that sooner or later the consumers will prevail by voting with credit card against the worst systems" – the same conclusion which INDICARE has drawn in its State-of-the-Art Reports. There-

fore beside the experiments carried out underlying the findings, there is nothing really special in the report that DRM experts were not aware of.

So I consider the main value of the research is that it is easy to read for the public, and comes to the right conclusions, therefore educating consumers about today's DRM systems limitations – and also on how to exercise their wish for interoperability by circumventing content protection.

Sources

- BEUC, (2005): Test on interoperability between online music stores and portable players – Summary. BEUC http://www.consumersdigitalrights.org/mdoc/x045cku2005e_13993.pdf
- Consumer Digital Rights web site, (2005): http://www.consumersdigitalrights.org/
- Intertek, (2005): Technical Report – Online Music Download Services. BEUC http://www.consumersdigitalrights.org/mdoc/OnlineMusicDownloadServices_TechnicalReport_90041.pdf

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 21/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=163

First steps towards an open standard for a content protection and copy management system from the DVB

By: Chris Hibbert; Chairman, DVB-Copy Protection Technologies Group, London, UK

Abstract: After five years of work the Digital Video Broadcasting Project has published the first elements of its specification for a Content Protection & Copy Management (DVB-CPCM). This article introduces the background of DVB, explains rationale, scope and concepts of CPMC, and finally outlines next steps.

Keywords: review - authorised domain, broadband, conditional access, content protection, digital TV, interoperability, stakeholders, standards, usage rights

Introduction

In November 2005 the Digital Video Broadcasting Project published a Blue Book, A094, containing the first three elements of its specification for a Content Protection & Copy Management (DVB-CPCM) system for use in consumer digital products and home networks.

The first three elements of the DVB-CPCM specification are: the CPCM Reference Model, which provides a technical and architectural framework for the CPCM System; the CPCM Usage State Information, which is content metadata that signals the authorised usage for a particular Content Item; and CPCM Abbreviations, Definitions and Terms.

Although the full system specification for CPCM is not complete the Blue Book is published for informational purposes and liaison with other interested standards forums. When completed the DVB-CPCM specification will be submitted to ETSI for standardisation.

This article will not go into a detailed description of the full functionality offered by DVB CPCM as the reader can obtain the Blue Book by download from the DVB web site (DVB 2005). Rather the following is intended to give background to the DVB, why it embarked upon the work, and the major concepts embodied within the specification.

About the DVB

Today, the Digital Video Broadcasting Project (DVB) is an industry-led consortium of approximately 300 broadcasters, manufacturers, network operators, software developers, regulatory bodies and others committed to designing open standards for the delivery of digital television and data services. Although based in Europe DVB has members in over 35 countries.

The genesis of DVB was the debacle following the market failure in the early 1990's of the D-Mac satellite system which was mandated by the EC administration but not supported industry wide in Europe.

Persisting in the belief that pan-European standards for digital broadcasting will bring major benefits to consumers and manufacturers, the European Community administration turned to the industry and encouraged the setting up of a cross industry group to produce open specifications for standardisation based on industry consensus. This led to the formation of the DVB Project in 1993.

Initially the DVB concentrated on producing specifications for digital transmission systems for satellite, cable and terrestrial delivery and an interoperable Conditional Access system. These specifications have been adopted on a world wide basis resulting in the DVB becoming accepted as one of the leading specifications bodies. In recent times DVB has moved into the area of middleware and software producing the Multimedia Home Platform specification for interactive content and the Portable Content Format to provide common authoring to non-interoperable interactive platforms. Recently completed specifications also include DVB-H for broadcast delivery to hand held devices, DVB S-2 an updated and more efficient system for satellite delivery than its first specification which is now ten years old. Work is ongoing within DVB on advanced encoding technologies and IPTV.

Since its inception the DVB Project has proven the value and viability of pre-competitive cooperation in the development of open digital television standards. DVB open standards guarantee fair, reasonable and non-discriminatory terms and conditions with regard to Intellectual Property Rights, allowing them to be freely adopted and utilised worldwide. Open standards guarantee that compliant systems will be able to work together, independent of which manufacturer provides the equipment enabling considerable economies of scale to the benefit of the industry and also the consuming public.

The DVB is market lead. Its technical specifications are written to strict commercial requirements established by consensus by its members which represent all the industry constituencies of interest and the consumer through CE and IT vendors and broadcasters who have an interest in only producing products which are compelling and affordable.

Why DVB CPCM?

In the late 1990's visionaries in the DVB predicted that the future growth of digital distribution of video and audio content; the advent of affordable consumer digital recording and processing equipment and software; and the potential for easy content movement by peer-to-peer transfer via broadband connectivity, would turn the existing consumer content usage paradigm on its head. Whilst convenient for consumers, the ease of unrestricted re-distribution of commercial content and associated loss of revenue to the content creation industry would reduce the income needed for investment in new content. The inevitable reaction of the content industry would be the push for DRM and content protection technologies in consumer products. On the other hand, a degree of content usage control, where applicable, would encourage content providers and distributors to introduce compelling new consumer propositions enhancing digital home networking and storage.

It was therefore logical that DVB should embark upon an attempt to produce a specification for digital content protection and copy management to complement its other work in emerging new platforms. Interested DVB members determined to attempt to provide an open standard CPCM system specification for use in consumer products which, if adopted, will avoid a plethora of non-interoperable proprietary systems resulting in higher costs and consumer confusion so

slowing digital take up and hindering moves towards analogue switch-over.

In September 1999 the DVB established a new commercial sub-group within its Commercial Module with a mandate to prepare Commercial Requirements for a CPCM system to provide a common framework for the protection and management of commercial content in consumer digital equipment and home networks whilst taking into account consumer interests such as; no requirement for system registration or a return path; simple to use with clearly displayed information about usage rights.

The group spent three years deriving the Commercial Requirements for CPCM which indicates the degree of difficulty in reaching consensus across the industry in the emotive area of content protection.

Inevitably viewpoints were initially somewhat polarised across the industry sectors. For example, there was clearly a need to balance the concerns of the rights owners to protect their revenues with the concerns of the consumer electronics industry to protect the investment made by their customers in purchasing equipment. Public Service broadcasters were concerned that signalling over restrictive use of their broadcast content would conflict with their public service charters. Pay TV broadcasters were looking for a means to integrate CPCM with existing Conditional Access systems to support new commercial offers such as VoD (video on demand). However, despite these differences, consensus was finally achieved by participants recognising and accommodating each other's business models.

In 2001 the Commercial Requirements for CPCM were approved by the Steering Board of the DVB and a sub group of the Technical Module was set to work to produce the specification.

The CPCM system

Although the functionality targeted for DVB-CPCM is much less ambitious than that of a full digital rights management (DRM) system, the scope envisaged is for end-to-end protection of commercial digital Content in all processes from the point of acquisition by the consumer through to the point of consumption.
Possible sources of commercial digital Content include broadcast (e.g., cable, satellite, and terrestrial), Internet-based services, packaged media, and mobile services, among others.

It is also intended that DVB-CPCM shall be applicable to the widest range of equipment encompassing in-home digital networks, personal digital recorders; in the home and portable, and facilitate remote connectivity to other locations such as a second home or a vehicle.

CPCM is intended to be used to manage all types of commercial Content - audio, video and associated applications and data delivered to consumer devices from acquisition until final consumption, or export from the CPCM system. Allowed usage is signalled by Usage State Information (USI) in the form of metadata which is securely bound to the content.

USI has been designed to accommodate a variety of business models and regulatory regimes. The existence of any particular field of USI in the specification does not imply that it will be asserted in a particular instance, or that it will be allowed to be asserted. Details regarding how and by whom a USI field can be asserted or changed will be reflected in the relevant CPCM compliance regime, which is outside the scope of the specification. For instance, European Public service broadcasters are indicating that they are considering setting a profile of CPCM USI signalling such that content scrambling should not be applied and that the only restriction required is to inhibit the re-transfer of the Content by means of the Internet.

CPCM is intended to interface with DVB Conditional Access (CA) systems and, where required, free-to-view broadcast delivery networks. It was recognised that DRM and copy protection systems already exist in the marketplace and will continue to be used and developed. Hence to the extent possible, without compromising its integrity and security, DVB-CPCM must co-exist with and

interoperate with other DRM and copy protection systems.

The Authorised Domain

The DVB recognised that to conform with the traditional user experience of home recording, the portability of pre-recorded content, and expectations based on emerging digital connectivity, it was necessary to identify a mechanism to replicate the reasonable boundaries of content movement consumers have come to expect whilst not limiting the advantages of new digital technology. Based on the above, the concept of a user "Authorised Domain" was developed.

The Authorised Domain is defined as a distinguishable set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household. A household is considered to be the social unit consisting of all individuals who live together, as occupants of the same domicile. This makes no assumptions about the physical locations of the devices owned, rented or otherwise controlled by the members of the household and no mechanisms to identify and/or authenticate the user shall be required.

A CPCM device may only be a member of one Authorised Domain at any time. When signalled by USI, Content is constrained to the Authorised Domain by which it is acquired and will not play on a devices belonging to a different Authorised Domain. However, to allow flexibility of connection a device can be re-assigned to another Authorised Domain for the purpose of consumption of Content assigned to that Domain during which time it cannot access Content which was bound to its original Authorised Domain. There is no limit to the number of times a device may move between Domains as long as the Content-to-Authorised Domain binding is maintained.

The specification provides mechanisms to determine the size and scope of the Authorised Domain; such size and scope to be decided by the implementer and possible local regulation.

DVB-CPCM can also be used to constrain Content to the local environment into which it is delivered by broadcast, if so signalled by the USI, to support local rights assigned to the broadcaster. The local restriction can be lifted after a defined period of time or the end of the transmission.

It should be emphasised again that provision of this mechanism does not mandate content distribution restriction in all cases. The USI will convey the restriction of movement within the Authorised Domain when it applies. If the restriction is not signalled by USI then the user will be allowed to send the content "outside" the Authorised Domain. It is envisaged that there will be many cases where the content owner or distributor will wish this to happen.

End-to-end protection & interoperability

A guiding principle in the development of CPCM is that implementation should not be dependant on a single technology. Rather, CPCM should provide a framework for interoperability between competing technologies. This enables a range of competing technology providers to collaborate to achieve a specification for a system which, whilst providing interoperable transfer of content between devices from a choice of providers, ensures that consumers can purchase equipment from different manufacturers in a competitive market and be assured that the equipment will inter-operate.

DVB-CPCM is intended for deployment in individual devices and in home networks. A content scrambling algorithm and secure exchange mechanism will be specified to preserve the security of the CPCM system. CPCM Content will only transfer between devices which are fully DVB-CPCM compliant, can establish mutual trust, and obey the USI. Intermediate devices, or entities such as network architecture items and storage on hard drives or removable recordable media, should be transparent because the Content and USI is secure. This approach increases security and ease of implementation by avoiding the necessity of multiple decrypt and re-encrypt processing as would be the case if each entity, device or linkage, comprising a home network was to use incompatible security mechanisms. It also reduces the need for multiple cross-licensing.

Next steps

The DVB Technical Module sub group is working to produce the specification for the security elements, to fully technically define the characteristics of the Authorised Domain, and the means to securely bind content within its boundaries. It is hoped that these final elements of the CPCM system specification will be published by mid-2006, along with Implementation Guidelines which will give examples of the use of CPCM in a number of markets and business models. Guidance will also be provided on the scope of technical testing required to ensure interoperability and compliance.

Cross industry support

Although CPCM is probably the most contentious work item the DVB has attempted the process has received input and support from, typically 25 to 30 member companies from across the industry constituencies of interest with representation from major technology providers.

Inevitably there is likely to be criticism, even from some DVB members, of the development of any form of content protection in consumer products and accusations that DVB CPCM will limit the availability of content to consumers. But the majority of DVB members believe there is a growing market need for content protection and copy management and that the DVB history of an inclusive, open consensus building approach provides the best option for development of a specification which will provide tools with wide ranging options.

Some critics have accused the DVB of conducting this work "behind closed doors". Whilst it is true that the DVB is a member organisation, it is open to any organisation or company which wishes to participate and is willing to contribute its intellect or technology to the benefit of the industry at large. Membership requires the signing of the DVB Memorandum of Understanding which requires this commitment.

Sources

- DVB (2005): Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) System. CPCM Reference Model. DVB Document A094, November 2005; http://www.dvb.org/index.php?id=294

Acknowledgement: This significant work which started five years ago has been supported by a broad representation of DVB members from all the constituencies of interest; content providers, broadcasters, distribution platform operators, consumer product manufacturers, and technology providers. As can be imagined content protection in consumer products and some free-to-air broadcast markets is a potentially contentious issue. It has therefore taken some time to embrace the concerns of all the players in the market and for all the parties to reach a level of understanding of each other's present and future business models.

The author therefore acknowledges the work of all colleagues in the DVB commercial and technical sub-groups.

About the author: Chris Hibbert is Vice President Media Technologies & Standards with Walt Disney Television International. He was formerly Director of Engineering with ITV Digital in the UK during which time he became chairman of the DVB CPT group. Previously as Director of Engineering for the ITV Network he was responsible for technical strategy for DTT and was a member of the DVB group which wrote the requirements for the DVB-T specification. Hibbert is a member of the DVB Steering Board, has played an active role in the TV-Anytime Forum and is a fellow of the Royal Television Society. Contact: chris.hibbert@disney.com

Status: first posted 13/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=159

DRMTICS 2005 – a truly interdisciplinary forum for DRM research. A conference report

By: Wanqing Li, Rei Safavi-Naini and Nicholas Sheppard, University of Wollongong, Wollongong, Australia

Abstract: The First International Conference on Digital Rights Management: Technology, Issues, Challenges and Systems (DRMTICS 2005) took place in Sydney from October 31 to November 2. It was the inaugural conference in an annual series covering research in all theoretical and practical aspects of digital rights management systems. The conference series serves as a broad multi-disciplinary forum for all DRM-related issues, including expression of rights, processes, methods and systems for enforcement of rights, DRM applications, together with the social, legal, usability and business aspects of DRM systems.

Keywords: conference report – copyright law, digital TV, DRMS, P2P, rights expression language, technical protection measures, trusted computing

Introduction

DRMTICS 2005 (pronounced: "dramatics") was the inaugural conference in a series considering all aspects of DRM systems including issues faced by holders of digital rights who want to protect their intellectual property rights and consumers who seek to protect their privacy and to preserve their traditional pattern of access to media under existing copyright law.

The conference attracted submissions from all of Asia, Australia, Europe and North America, from which twenty-seven papers were selected for presentation at the conference. The programme also included three invited speakers and a panel session. The papers covered a variety of topics, including cryptography, digital watermarking, legal issues, rights expression languages, trusted computing and complete digital rights management frameworks.

DRMTICS 2005 was held in co-operation with IACR (International Association for Cryptologic Research; cf. sources) and the IEEE Computer Society Task Force on Information Assurance (cf. sources), and sponsors included electronics giant Motorola The full proceedings of the conference will be available in Springer's Lecture Notes in Computer Science series (DRMTICS 2006) in 2006.

Invited talks

The three invited talks were given by *Renato Ianella* (NICTA, Australia and ODRL Initiative), *Moni Naor* (Weizmann Institute of Technology, Israel) and *Karen Gettens* (Blake Dawson and Waldron, Australia).

Renato's talk focused on the evolution of rights expression languages (RELs) from the late 90's with DPRL up to Creative Commons and focusing on the ODRL REL. He looked at the standardisation of RELs and the impact this has had where successful, such as the mobile sector with the Open Mobile Alliance DRM specifications and concluded by reviewing the current "DRM Patents Saga" that has plagued the standardisation effort. He raised the issue of the applicability of some of the patents to RELs and the serious impact this will have on future research in this area, and the direct impact to systems being deployed today.

Moni surveyed some proposals for designing cryptographic schemes that take into account both human and computer abilities and weaknesses in solving various types of problems. These include schemes for traditional cryptographic tasks such as identification, authentication and encryption, as well as more modern ones, such as spam and abuse prevention, denial of service and voting.

Karen gave an overview of legal action taking place in the digital rights management world. She took us through the subtleties of the legal decisions in

- the *Sony vs Stevens* mod-chipping case in Australia;

- the *MGM vs Grokster* file-sharing network case in the United States; and
- the Universal Music vs Sharman Networks (Kazaa) case in Australia.

Karen concluded that courts have generally sought a balance between copyright owners and other parties, to the point of creating principles that are not included in the law itself. She further concluded that the particular outcomes in the file-sharing cases are very fact-specific and do not represent broad decisions for or against peer-to-peer technology.

Rights Expression Languages

A new rights expression language is being developed by the Audio Video Coding Standard Working Group of China. This was to be presented by *Ying Sha* (Chinese Academy of Sciences, China), but he was unable to travel to Australia and was represented by compatriot *Bin Zhu* (Microsoft Research Asia). *Kurt Maly* (Old Dominion University, USA) presented a comparative study of two languages not widely considered in the digital rights management literature, the eXtensible Access Control Markup Language (XACML) and the Policy Core Information Model (PCIM).

Paul Koster (Philips Research, the Netherlands) proposed to introduce "user-attributed rights" that allow users to control the way content which has been purchased is shared amongst their family, friends, etc. without interfering with the rights of the original content owner.

Legal and social aspects

Brian Fitzgerald (Queensland University of Technology, Australia) presented further details of the *Sony vs. Stevens* case. This case addresses the question of whether or not region-coding devices -- such as those used in the Sony PlayStation -- are to be considered "technological protection measures" under copyright. Current case law in Australia holds that they are not, but Fitzgerald warns that amendments guided by the recent Australia-US Free Trade Agreement may result in unforeseen control over the use of products being handed to multi-national corporations.

Yee Fen Lim (Macquarie University, Australia) also argued that digital rights management systems and the laws that support them increase the rights of copyright owners beyond what they are given in copyright law, to the point of creating an intellectual property regime even more powerful in some respects than that for tangible property.

Supriya Singh (Royal Melbourne Institute of Technology, Australia) and *Jenine Beekhuyzen* (Griffith University, Australia) gave an entertaining presentation disputing record companies' claims that music fans use free downloading as substitute for purchase. Their series of interviews with Australian music fans demonstrated a continuum in behaviour between free downloading and purchase: most interviewees combined freely-obtained and purchased music depending on a variety of factors including the availability of their preferred forms of music, their financial means and their level of familiarity with a particular artist.

Panel session

The panel session brought together technical and legal minds to discuss the subject *Is Reliable and Trusted DRM Realistic or Even Possible?* Discussion could no doubt continue almost indefinitely on such a provocative topic but we had to discuss what we could in an hour.

The panel was chaired by *Bill Caelli* (Queensland University of Technology, Australia). *Ezzy Dabbish* (Motorola, USA) and *Bin Zhu* (Microsoft Research Asia) presented the technical side, while the legal view was represented by *David Vaile* (Baker & Mackenzie Cyberlaw and Policy Centre, Australia), *Philip Argy* (Mallesons Stephen Jaques, Australia) and *Susanna Leisten* (Queensland University of Technology, Australia).

It seems fair to say that the general view of the technical community involved is that DRM systems will exist and their reliability and trustworthiness will be possible within certain parameters – no security system will ever be perfectly secure in itself, but it can be secure enough to serve its purpose given the right legal and other support.

The views of legal side were less unified. While Leisten outlined the negative effects of strict regimes for protection of digital rights, Argy viewed DRM systems as a natural evolution of property protection systems. Vaile questioned the possibility of DRM systems that can provide fair use.

Cryptography

Broadcast encryption has become an important cryptographic primitive for conditional access and digital rights management systems. *Miodrag Mihaljević* (Serbian Academy of Science and Arts) presented one paper describing potential weaknesses in certain broadcast encryption schemes, and another describing a new scheme with improved efficiency and greater security than previous schemes. *Ulrich Greveler* (Ruhr University Bochum, Germany) presented a new scheme offering unconditional cryptographic security at the cost of allowing a few free-riders.

Jacques Fournier (GEMPlus S.A., France) showed how cryptographic operations can be vectorised for efficient implementation on embedded systems such as smartcards.

Tamper-resistance

The security of digital rights management systems depends on the inability of attackers to reverse-engineer and modify sensitive hardware and software components. *Mahadevan Gomathisankaran* (University of Iowa, USA) presented an architecture for verifying the correctness of systems without requiring the verifier itself to be given sensitive information about the system. *Brian Blietz* (University of Iowa, USA) presented a software tamper-resistance system based on extending the power of small, heavily-obfuscated process to a larger process that performed the real function of the software. *Valery Pryamikov* (Harper Security Consulting AS, Norway) presented a new method of preventing reverse-engineering of software based on transforming a programme's function call tree.

Watermarking

Watermarking continues to be one of the active research topics with extended applications from multimedia security to software security. *Hongmei Liu* (Sun Yat-Sen University, China) presented two papers. One is about a scheme for reversible semi-fragile image authentication that is able to locate any tampered areas but is tolerant to JPEG compression. Another is DC coefficient-based video watermarking compliant to MPEG-2 bit stream without any additional payload. *Yongwha Chung* (Korea University, Korea) presented a case using robust and fragile watermarking (dual watermarking) for the communication of fingerprints. The robust watermark may be used to identify source devices. *Clark Thomborson* (University of Auckland, New Zealand) introduced software watermarking as a means of preventing software from piracy and unauthorised modification and presented an improved version of the QP algorithm through register allocation.

Systems

The last day of the conference was mostly given over to proposals for complete digital rights management systems. *Bin Zhu* (Microsoft Research Asia, China) presented two systems, one for a privacy- and copyright-respecting peer-to-peer network and another for scaling the quality of content according to the user's willingness to pay for it. Another copyright-respecting peer-to-peer service was presented by *Kyung-Hyune Rhee* (Pukyong National University, Korea).

Ulrich Greveler (Ruhr University Bochum, Germany) discussed several methods of enforcing regional access to pay-TV broadcasts and concluded that, even though deployment of trusted hardware is considered the standard requirement for digital rights management systems, trusted hardware was not necessarily the best solution in this scenario.

Bottom line

DRMTICS provides a forum where all researchers from all disciplines with an interest in digital rights management can come together and share their views and ideas. While technical presentations decidedly outnumbered the other presentations at this year's conference, both technical and non-technical disciplines were well-represented amongst the conference delegates. As noted

in another INDICARE conference review (Kerényi 2005), a healthy exchange between the technical and non-technical communities is essential to successful deployment of digital rights management. Hopefully DRMTICS 2005 represents a good start to a significant event on the annual DRM calendar.

Sources

- DRMTICS Conference Page: http://www.titr.uow.edu.au/DRMTICS2005/
- DRMTICS (2006): Proceedings will be available in Springer's Lecture Notes in Computer Science series; http://www.springer.com/lncs
- IACR (International Association for Cryptologic Research): http://www.iacr.org
- IEEE Computer Society Task Force on Information Assurance: http://www.ieeeia.org
- Kerényi, Kristóf (2005): DRM researchers do not disregard consumer acceptability any more: http://www.indicare.org/tiki-read_article.php?articleId=157

About the author: Rei Safavi-Naini is a Professor in computer security at the University of Wollongong, Australia and is the Programme Chair of DRMTICS 2005 as well as the ACM Workshop on Digital Rights Management 2005. Contact: +61 2 4221 3800, rei@uow.edu.au. Wanqing Li and Nicholas Sheppard are academic staff at the University of Wollongong and are the General Co-Chairs of DRMTICS 2005. Contact: +61 2 4221 5410, wanqing@uow.edu.au and +61 2 4221 3788, nps@uow.edu.au.

Status: first posted 15/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=160

Axmedis plus = technology + users + consumers

By: Gergely Tóth, SEARCH Laboratory, Budapest, Hungary

A report on the 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution (Axmedis 2005)

Abstract: INDICARE was present at the Axmedis 2005 Conference in Florence from November 30 to December 2. The conference was organised by the Axmedis project, aiming at bringing together representatives of different fields related to cross-media. Besides the traditional scientific and industry-inspired talks, presentations focusing more or less on the consumers' point of view (e.g. interoperability or consumer protection) found their way into the programme.

Keywords: conference report - business models, collecting societies, DRMS, EU project, interoperability, privacy, standards, stakeholders, users

Introduction

The Axmedis project (cf. sources) aims at reducing the cost of cross-media production and distribution, at searching for and integrating objects and components and at managing and monitoring distribution. Axmedis is an integrated project (IP), funded by the European Commission under the 6th Framework's Information Society Technologies (IST) programme, with *Paolo Nesi* from the University of Florence as its co-ordinator. Since the project specifically aims at developing and providing methods and tools for innovative and flexible Digital Rights Management, it is particularly relevant concerning INDICARE.

To fulfil its objectives the project organized the Axmedis 2005 Conference with the title *1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution* in Florence from November 30 to December 2, 2005. The three-day conference provided a rich programme. The speakers came from a wide range of organisations, thus researchers, delegates from industry, regulators and also consumer representatives were present. During the course of the conference one uncer-

tain trend seemed to visualize for me: besides the regular scientific-, business- and industry-oriented issues, consumer-related talks could also be heard. Whether this marks the process of research and industry slowly taking the consumers' view and requirements into account or this was just the specialty of this conference and proof of the skills of the conference organisers remains to be seen.

On the first day after the welcome speeches an invited talk started the conference. Afterwards the programme continued in three or even four parallel sessions. Besides the core Axmedis subjects including an Axmedis tutorial track throughout the conference and the "Axmedis Call for take up action", there was a panel on "The role of collecting societies in the digital era" (see later), an extensive MPEG Workshop, a special session of the EUAIN project (see later) and in addition the 3rd Virtual Goods Workshop, which was co-located with the conference (see later). By this approach it was possible to address the subject matter not only from a technological point of view but from the point of users and consumers too. The whole programme is available at the homepage of the conference and all papers are available in the conference proceedings (Nesi et al. 2005).

Due to this huge programme, I was not able to attend all presentations, thus the following report will just be a subjective glimpse of the whole event. Nevertheless it has to be stated that the organisers did their best with the conference and the event progressed smoothly.

Invited talk

After the welcome talks the conference started with the invited talk by *Leonardo Chiariglione* from the DMP project (cf. Jeges and Kerényi 2005). In his talk Chiariglione argued that the protection of intellectual property should be in balance with its use. Nowadays, when analogue is shifting to digital and thus the challenge of managing scarcity is changing to managing abundance he proposed a *rational* DRM architecture, which is both scalable and interoperable and composed of standard technology and equipment.

Security of DRM

That Axmedis successfully brought together parties with different goals and backgrounds and that such presentations can form a symbiotic whole (even following up Chiariglione's vision of a rational DRM) were clearly illustrated by the next two talks given during the Content Security and Digital Rights Management session.

Josep Domingo-Ferrer presented a solution on multicast fingerprinting and collusion security. The main challenge solved was to equip multicast content with unique fingerprints, thus copy detection could be used complementary to copy prevention. This solution, which could find support in the technology domain, naturally is objectionable from the privacy (and thus the consumer's) point of view (cf. presentation by Grimm later).

On the other hand *Jose Prados* explored the possibilities of interoperability of rights expression languages (RELs) and protection mechanisms. In particular he analyzed how the REL of OMA DRM 2 (cf. sources), i.e. ODRL (cf. sources) , and that of MPEG-21 (cf. sources) could be converted into each other. While the presentation focused mainly on technical issues, interoperability, i.e. to rightfully consume protected content on any device was highlighted as one of the main consumer requirements for DRM.

Collecting societies

The panel session "*The role of collecting societies in the digital era*" provided an interesting insight into the challenges these organisations face with the switch to the digital content gaining momentum in the 21st century.

Maila Sansaini from IMAIE analysed DRM from the point of view of a collecting society. While DRM can protect against privacy by applying technical measures, helping in identifying works and allowing payment for the content it still has deficiencies: current solutions are not interoperable; they do not ensure equal remuneration of copyright and neighbouring rights holders and can also be cracked.

Dominic McGonigal from PPL, UK, did not analyze DRM, he rather chose the approach of introducing the operation and problems of a collecting society to the audience. By describing the internal processes of his organisation, how the huge volume of music content is managed, how licences are stored and usage information is processed in order to distribute income between producers and performers, DRM architecture designers could gain insight into the life of a potentially important DRM system user.

Accessibility

Another session focusing mainly on the consumer was related to the interconnection of DRM and accessibility. This track was assigned to EUAIN, the European Accessible Information Network (cf. sources).

In the first talk *David Crombie* introduced the core idea behind EUAIN. He emphasized that current practice is to apply quick fixes to fill the gaps in order to achieve accessibility, while in the long term accessibility can only be achieved if it is managed as a process throughout the life-cycle of a product. This change of mind is promoted by EUAIN, and IST-funded project to promote eInclusion as a horizontal building block in the establishment of the information society.

Roger Lenoir continued by exploring the possibilities and achievements of open software and open standards as tools for accessibility. In his presentation he compared the associations representing visually impaired people with the open source communities, where in both cases voluntary work dominates. Finally, Lenoir introduced some current projects (DAISY, NIMAS, WCAG) focusing on accessibility.

Virtual Goods Workshop

This year the Virtual Goods Workshop was co-located with the Axmedis 2005 Conference. This series of workshops focuses on the multi-disciplinary assessment of existing DRM technologies and business models. Unfortunately I could not attend the whole workshop, only the first part, thus the following is a partial overview of this year's event.

In his presentation *Stephen Saunders* evaluated the current shift in the music industry from distributing music through retail stores towards the thousand-faceted digital distribution. His argument was that it was high time to start to change the way music is regarded: industry should move from thinking of music as a good to using it as a service with different service levels for different users.

Prof. Rüdiger Grimm, University of Koblenz (formerly at TU Ilmenau) introduced the results of an analysis aiming at evaluating privacy issues during DRM usage (Grimm et al. 2005). Although DRM systems' main goal is to enforce copyright, they are sometimes also used for recognition of bad behaviour, to deliver personalized watermarks and other technological methods interfering with privacy. Grimm presented results of data flow evaluations with concrete DRM architectures before completing a deal, at checkout, while checking the right during consumption, through special services and even through hidden interfaces.

Another presentation, given by *Matthias Spielkamp* from iRights.info strengthened the consumer representation at Axmedis. He introduced this German organisation which aims at delivering information about legal aspects of DRM to the consumers. The main goal is to inform the users about the legal background of typical use cases (e.g. downloading content from a peer-to-peer network or ripping a CD) in an independent way.

Bottom line

The Axmedis 2005 conference presented a good mix of research- or industry-driven and consumer-oriented talks. Although the project itself was mainly technology focused, the organisers did a great job in inviting a broad spectrum of presenters. As an advocate of the INDICARE project who is always looking at the end-users' point of view when it comes to DRM and generally to multimedia-relates issues, I am looking forward to the next Axmedis conference in December 2006 to see whether the shift towards a more consumer-centric view will further evolve. Could it be that this conference marked the start of a larger trend? I do hope so.

Sources

- Axmedis project: http://www.axmedis.org
- Axmedis 2005 conference: http://www.axmedis.org/axmedis2005/
- Digital Media Project (2005): http://www.dmpf.org
- European Accessible Information Network: http://www.euain.org/modules/wfsection/
- Grimm, Rüdiger et al. (2005): privacy4DRM Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management: http://www.datenschutzzentrum.de/drm/privacy4drm.pdf
- iRights.info – Urheberrecht in der digitalen Welt: http://www.irights.info/
- ISO/IEC JTC1/SC29/WG11/N5231 MPEG-21 Coding of moving pictures and audio: http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
- Jeges, Ernő and 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
- 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, 2005
- ODRL: http://www.odrl.org/
- Open Mobile Alliance – Digital Rights Management V2.0 Candidate Enabler: http://www.openmobilealliance.com/release_program/drm_v2_0.html

About the author

Gergely Tóth is a PhD student at the Budapest University of Technology and Economics in the SEARCH Laboratory. Besides Digital Rights Management his core interests include security and privacy. You can contact him at gergely.toth@mit.bme.hu

Status: first posted 20/12/05; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=161

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.

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