INDICARE Monitor

About Consumer and User Issues of Digital Rights Management Solutions

www.indicare.org ISSN 1614-287X

INDICARE Monitor Vol. 2, No 11, 27 January 2006

Content

Editorial 2
Knud Böhle, ITAS, Karlsruhe, Germany

Digital rights management and people with sight loss 4
David Mann

Trusted intermediaries are key to accessible content delivery 8
David Crombie, Roger Lenoir, David Mann, Neil McKenzie

Digital rights management and accessibility 12
Zoltán Nagy

DRM interoperability and reusability through a generic software architecture 16
Sam Michiels, Koen Buyens, Kristof Verslype, Wouter Joosen and Bart De Decker

DRM for digital broadcasting in Japan 21
Kiyohiko Ishikawa

The Sony BMG rootkit scandal
Consumers in the US finally wake up. And march to courts 25
Natali Helberger

Masthead 30

Editorial of INDICARE Monitor Vol. 2, No 11, 27 January 2006

By: Knud Böhle, ITAS, Karlsruhe, Germany

Abstract: The special focus of this issue is on *DRM and accessibility*, an important topic not only for blind, partially sighted and other print disabled people. Three articles complementing one another explore the technical, legal, and policy dimensions of accessibility and present the state of the art. Further articles deal with a layered architecture for DRM, DRM in Japan's digital broadcasting services, and Sony BMG's DRM in the light of the class actions filed against the company.

Keywords: editorial – INDICARE

About this issue

DRM and accessibility

The issue's special focus is on DRM and accessibility - an important topic not only for disabled persons. This topic has already been dealt with before in the INDICARE State of the art report by *Bettina Krings* (cf. Helberger et al. 2004, pp. 30-33) and in the first supplement to this report by *Ulrich Riehm* (cf. Helberger et al. 2005, pp. 6-8).

Disabled persons, especially blind, partially sighted and other print disabled people have to rely on exemptions within copyright law allowing them to effectively use assistive technologies even in cases where the content is protected by TPMs. The three articles dealing with this subject make us aware of the troubles still existing, but also of the solutions at hand. When talking about this subject it is important to have in mind that blind and visually impaired people are consumers like you and me, and that improving accessibility is not only to the benefit of this group, but for all of us.

David Mann, who works for the Royal National Institute of the Blind in the UK and chairs the European Blind Union's Working Group on Copyright and Publishing, provides an excellent overview of the issues at stake. Among others he points to the risk that DRM might disable assistive technologies and hints at the irony that the great potential of the e-book technology, enabling the accessibility of publications as never before for print disabled people, might not be leveraged due to DRM restrictions in place. He discusses in more depth Adobe's policy in this matter presenting it as a model where access to content is granted based on trust relationships and a trusted environment. Mann also points out that the EU in its copyright directive at least – in contrast to WIPO - recognises exemptions and limitations for people with reading related disabilities. However he criticises that it falls short of providing for the harmonization of the exceptions required.

The next article stems from *David Crombie* and colleagues who are co-ordinating the European Accessible Information Network (EUAIN), a project funded by the European Commission under the 6th Framework IST programme's *eInclusion* thread. Their article puts forward two important messages:

- First, by and large technological solutions and standards required to allow print disabled people to enjoy e-content are already there (not excluding however a series of problems still around). The crucial point is that solutions developed anyway for multi-channel publishing and reuse of electronic material can also be applied for accessibility publishing. Even more, accessibility publishing may be regarded as the basis for e-content publishing in general. This turns around the logic in an important way: what is required to serve communities with special needs may change from an additional ex post activity to a prerequisite of mainstream e-content publishing.
- Second, following the authors, in order to serve disabled people, trusted intermediaries and secure environments are necessary. In more general terms this approach might suggest that all groups or communities benefiting from copyright

exceptions would have to turn into authorized consumers in trusted environments. Hence copyright legislation – allowing the application of TPMs to protect content on the one hand, while stipulating exemptions on the other hand – might imply a push for trusted computing infrastructures.

The third article of the focus theme comes from *Zoltán Nagy*, Speech Technology Ltd, Budapest. It gives an overview of the state of art of assistive technologies for the visually impaired, in particular OCR, text to speech engines (TTS), and screen readers. In terms of applications the development of e-books from simple voice books to standardized "DAISY books" is sketched. These are digital talking books combining and synchronising text and high quality voice. Many books have been published using the DAISY standard which confirms that solutions developed for print disabled have the potential to become mainstream. Another interesting service, called Világhalló, has been developed in Hungary. It is an integrated *on-line* service which combines text and voice flow to consumers, a kind of text radio. Infringing copyright is made difficult as the text alone is not accessible. This is in line with the publishers' requirements as Nagy says.

This article makes us also aware that accessibility means more for blind and visually impaired people than mere e-book text to speech transformation. There is an urgent need for *websites* designed respecting accessibility criteria, a need for assistive technology supporting the use of *software*, and a demand to make high-devices and services like *mobile phones* more accessible. Addressing these challenges, the author also hints at possible solutions.

Technical analyses

Sam Michiels, *Koen Buyens*, *Kristof Verslype*, *Wouter Joosen* and *Bart De Decker*, computer scientists from the Katholieke Universiteit Leuven, Belgium, deal with a highly relevant topic: the lack of a generic software architecture guiding the design and implementation of DRM systems or applications, and supporting interoperability of DRM technologies and their reuse. In their view software architecture design for DRM should be at the top of the research agenda. The authors propose a layered DRM architecture that supports DRM developers in producing complete and interoperable systems. The architecture is approached from both a functional and a security perspective. What makes this article particularly readable for non-techies is the fact that the authors have taken the Internet architecture as a guiding model - not disregarding however the differences when it comes to DRM. What is also very laudable is that the developers did not exclusively discuss their own solution, but relate it to the efforts of others, in this case with those of the Digital Media Project, which has been addressed in the INDICARE Monitor several times already (cf. e.g. Jeges 2005).

The second technical analysis is about Japanese digital broadcasting. We invited *Kiyohiko Ishikawa*, researcher at Japan Broadcasting Corporation (NHK), to contribute to the INDICARE Monitor, and to help us compare different approaches of content protection in different regions of the world. The author, who is currently working on a security system for digital broadcasting based on home servers, introduces us to the current state of digital broadcasting in Japan and the protection measures in place. How it works in Japan is explained in some detail. Apart from the technical details, it is interesting to see the difference between the Japanese and the US approach. In Japan, where broadcasting is scrambled but free to air, the technical protection measures applied rely on a Conditional Access System (chipcard and set-top-box), which does not need a broadcast flag.

Legal analysis of the Sony BMG rootkit scandal

Natali Helberger analyses the Sony BMG rootkit scandal from a lawyer's point of view, i.e. she goes into detail with respect to the class actions filed against Sony BMG. A class action allows e.g. consumers to complain as a group avoiding individual law suits. One of these class actions was on behalf of Sony BMG CD buyers in the US and brought by a Californian lawyer, *Alan Himmelfarb*, while the second class action was brought by the Electronic Frontier Foun-

dation (EFF) with a broader scope: against Sony BMG's XCP technology *and* the MediaMax technology used by Sony BMG, *and* provisions in the consumer contract. An important observation is that in these cases it was consumer law (and not copyright law) brought against DRM.

Sources

- Jeges, Ernő (2005): Digital Media Project – Part I. Towards an interoperable DRM platform. INDICARE Monitor, Vol. 2, Number 4, June 2005; http://www.indicare.org/tiki-read_article.php?articleId=116
- Helberger, Natali (ed.); Dufft, Nicole; Groenenboom, Margreet; Kerényi, Kristóf; Orwat, Carsten; Riehm, Ulrich (2005): Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report – First supplement, Amsterdam May 2005; http://www.indicare.org/tiki-download_file.php?fileId=111
- Helberger, Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich (2004): 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

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 27/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=171

Digital rights management and people with sight loss

By: David Mann, European Blind Union, Lisburn, Northern Ireland.

Abstract: This article examines the barriers which digital rights management schemes can create for readers with sight loss, analyses some of the reasons for this, points to possible solutions and makes recommendations for further action by various parties.

Keywords: policy analysis - accessibility, disabled, e-books, EUCD, WIPO

1. Introduction

The European Blind Union (EBU) and its member organisations throughout the European Union are very concerned at the impact which digital rights management schemes can have on both blind and partially sighted people, and indeed others with a reading related disability such as dyslexia. We can be denied equal access to knowledge and culture if digital rights management schemes are inadequately designed or unfairly deployed.

Full and equitable access to information is essential if people with sight loss are to compete on equal terms in education and employment. It is also essential to full enjoyment of all aspects of daily life and of the potential advantages which modern technology brings. Voluntary agencies serving people with sight loss in member states devote significant voluntary resources to trying to ensure that blind and partially sighted people are not left behind by advances in communication, be it in the fields of broadcasting, telecommunications or publishing. This is an extremely challenging task, given the speed of development in these fields.

2. The issues for blind and partially sighted people

Blind, partially sighted and other print disabled people read electronic material by

modifying the way in which it is presented, without modifying the content. They may do this through magnification, transformation into synthetic audio, or the use of a temporary, or "refreshable" braille display. In some instances the software with which to make these changes is incorporated in mainstream packages, but the most flexible and adaptable solutions are achieved via dedicated "screen reader" software. The term "assistive technology" is used in this document to refer to this form of access.

Digital rights management schemes, or the technological protection measures within them, can react to assistive technology as if it was an illicit operation. Thus, the DRM systems applied to e-Books and e-documents can prevent access by people who use assistive technology to read the screen or to control the computer.

In those circumstances, the blind user is prevented from achieving the same degree of access as his sighted counterpart, or indeed any access at all.

A second problem can be the "disabling" of speech functions in a particular publication. While e-book readers may have the facility to reproduce synthetic speech, the rights holder can apply a level of security which prevents this from working. A person with sight loss can thus buy a book but find herself unable to read it.

We have been contacted by several people who have purchased e-Books from both major retailers and small publishers, only to find that they are unable to read them because of the way that the DRM has been applied.

For example, Lynn from London bought a Bible from Amazon, and found that the content was locked in such a way that she could not read it with her screen reader. She contacted Amazon who advised her to contact the publisher. Having taken this extraordinary step, she was told "there is nothing we can do about it".

EBU views this as discriminatory practice, as publishers are erecting barriers to access, however unwittingly. We do not believe there are commercial or technical reasons for this to continue.

This situation is in fact deeply ironic, since an e-Book can be a great way to make publications accessible to people who cannot read print. It is unsatisfactory and unnecessary because technology companies such as Adobe have actually taken steps to ensure that content can be protected and yet access still provided to disabled customers.

3. Technical analysis

Both Adobe Security and Adobe DRM can be configured to restrict the use of access tools such as screen readers. Typically, a commercial document or e-book in PDF format will have all accessibility features disabled. This is not the default position but is easily and most often selected by commercial publishers.

Microsoft e-book reader sells most of its titles with an "owner exclusive" level of security. In addition to having this "anti-piracy" function, the Owner Exclusive book also has use restrictions that apply to the legitimate owner of the e-book. In particular the text-to-speech capability that is built into Microsoft Reader for accessibility purposes is disabled. Similarly, "Owner Exclusive" limits use of the product to one device, which prevents a visually impaired user from downloading from a desk top PC to a more congenial device such as a lap top braille notetaker.

The objective of applying DRM to a piece of content is to define and implement the rules for the access to and use of that content. To achieve this, the DRM system has to operate in a controlled and trusted environment in which it is able to control all the options available to a user of the content.

This control requirement extends to accessibility tools – and explains the problems which have arisen in a conflict between DRM and accessibility. The Microsoft text to speech (TTS) synthesis tool has a broad functionality which is also incorporated in the Adobe Acrobat Reader. As a tool it is considered to pose a threat to DRM controlled content because of its broad functionality and because it does not connect in a trusted manner with the DRM system.

This is why the DRM system in the Microsoft e-Book Reader application blocks the

use of the TTS tool when the DRM is configured to manage the rights in premium (commercial) content. This was originally the default position with the Adobe Reader.

There are essentially two ways in which this problem can be addressed. The first is to set up a system where the DRM mechanism is able to recognise a trusted accessibility tool and then unblock access to content for that tool. The second way is by devising instructions, expressed through the rights expression language, which are available to authorised users of trusted access tools.

Adobe has already initiated a program incorporating the first approach. The DRM system used in the Adobe reader is now able to recognise and establish a trusted relationship with at least two accessibility tools (Window-Eyes and Jaws screen readers). Allowing access to DRM protected content is now reportedly the default position of the reader.

The effect of this trusted relationship between the Reader and the accessibility tools is that access (including text to speech) can be facilitated without in any way derogating from the security level applied to the content generally (e.g. no printing, no altering, no saving to alternate formats).

To achieve this relationship, third party applications are submitted to Adobe for testing the security and compatibility issues. To quote from Adobe's *Loretta Guarino Reid*, in a response to an enquiry from the RNIB "Techies" e-mail list dated 15th December, 2005: "Our solution depends on a special mechanism that vendors can use to identify themselves as trusted clients. To implement this properly really requires suitable operating system support to provide a secure channel to trusted client programs, and a good mechanism for validating the identity of the client program."

Thus the feasibility of access to Adobe DRM through assistive technology has been established, but effective realisation remains protracted and by no means universally rolled out.

The information of this chapter is drawn largely from "Accessing and Protecting Content", by Garnett, White and Mann (Garnett et al. 2005), a report prepared during 2005 by RNIB within the European Accessible Information Network Project (cf. sources) funded by the European Commission. We would also like to recommend an article entitled "The soundproof book", by George Kerscher, International Project Manager, DAISY Consortium, and Jim Fruchterman, CEO, the Benetech Initiative (Kerscher and Fruchterman 2002). Although written some time ago, this article has not lost its validity, and still poignantly illustrates the threats posed by DRM.

4. The legal background

International treaties have long permitted national legislatures to introduce exceptions and limitations to copyright in various circumstances, including exceptions and limitations for the benefit of people with a reading related disability. By no means all EU member states yet have such exceptions, and there is no consistency amongst the exception regimes that do exist.

Unfortunately, technological protection measures can negate these exceptions if they make it difficult or impossible to access material which one is entitled to read.

At international level, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) require, in Articles 11 and 18 respectively, legal protection for rights holders using technological protection measures. However, they make no specific provisions to protect the beneficiaries of exceptions to copyright whose access is blocked by such measures.

Individual member states and the European Union collectively will shortly be ratifying these treaties.

Fortunately, the European Copyright Directive (EUCD 2001) is more helpful. While it, too, seeks adequate safeguards for rights holders against the circumvention of technological protection measures, it does state in Article 6.4.1:

> "…in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties con-

cerned, Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned" (EUCD 2001).

Article 5.3.b is the one relating to exceptions and limitations for the benefit of people with a reading related disability. Hence the Directive envisages protection against technological exclusion for such users.

Again, there is no evident consistency in the way in which these provisions are being transposed into national law. It is ironic that a directive which has the word "harmonisation" in its title does nothing to harmonise exceptions to copyright or protection of the beneficiaries of those exceptions that do exist. The EUAIN project (referred to above) will be analysing the implementation across the EU of Article 6.4.1 and, if appropriate, making recommendations to the Commission on required changes.

It is essential that governments set up robust, effective and efficient procedures to allow print disabled people who find their access blocked by a technological protection measure to gain the access to which they are entitled. For legislation to permit circumvention in certain well-defined circumstances would be helpful. That alone, however, would not be the total answer, as the potential user might not have the necessary skills to circumvent. Arrangements for prompt legal or administrative recourse are also required.

As already noted, the European Union has recognised that copyright exceptions for disabled people may be compromised by the technological protection measures within DRM Systems. Subsequent to the passage of the Directive, both DG Information Society and DG Enterprise conducted work on DRM, the latter through CEN (Centre Européen de Normalisation). This work indicated that the whole issue remains fluid and largely untested, and that interoperability and protection of consumer rights are key issues which still need to be safeguarded.

5. Conclusions and recommendations

The access rights of people with sight loss have not yet been sufficiently recognised by politicians, standards bodies, content providers or the IT industry.

Governments and Parliaments have a duty

- a) to ensure that they have comprehensive and up to date provisions to ensure that accessible copies of all published material can be created without the requirement for rights holder permission; and
- b) to establish effective measures to give the beneficiaries of such exceptions immediate and equitable access to material from which they find themselves excluded by protection or rights management measures.

If such procedures can be achieved through voluntary agreement with rights holder groups they will probably work more smoothly, but legal backing for the right of access is essential in the interests of social inclusion and equitable treatment of people with disabilities.

The publishing and IT industries also have an important role to play. The developers of DRM schemes should apply principles of universal design. They must address the impact of DRM on readers using assistive technology, ensuring that such technology is recognised as legitimate and authorising appropriate manipulation of the way in which content is presented.

It is also in publishers' interests to ensure that the way in which their assets are packaged do not limit the number of potential customers.

Sources

- European Accessible Information Network (EUAIN): http://www.euain.org
- European Blind Union (EBU): http://www.euroblind.org/
- EUCD (2001): Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf
- Garnett, N.; Mann, D.; White, M. (eds.) (2005) : Accessing and protecting content. EUAIN consortium, FNB Amsterdam
- Kerscher, George; Fruchterman, Jim (2002) The soundproof book. Exploration of rights conflict and access to commercial eBooks for people with disabilities; http://www.daisy.org/publications/docs/soundproof/sound_proof_book.html
- Royal National Institute of the Blind (RNIB): http://www.rnib.org.uk/

About the author: David Mann, RNIB (Royal National Institute of the Blind), Chair, European Blind Union Working Group on Copyright and Publishing. David, himself visually impaired, works as a lobbyist for RNIB, the UK's leading voluntary agency for blind and partially sighted people. Previous experience includes managing the RNIB Talking Book Service and campaigning on copyright and related issues. Contact: David.Mann@rnib.org.uk

Status: first posted 26/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=170

Trusted intermediaries are key to accessible content delivery

By: Crombie, D., Lenoir, R., Mann, D. & McKenzie, N., EUAIN Network, Amsterdam, The Netherlands

Abstract: Much of the discussion around DRM and Accessibility has necessarily focused on the right of access versus the need to protect content. However, points of common interest exist and the development of *trusted intermediary* concepts can offer real-world solutions. The EUAIN network seeks to balance the needs of publishers and content providers with specialist organisations providing alternative format materials.

Keywords: accessibility, accessible content processing, disabled, inclusion, intermediary, publishers, trusted third party

Introduction

The European Accessible Information Network is a community of organisations and individuals who are examining new approaches to accessible content processing. The EUAIN network is funded by the *eInclusion* thread of the European Commission 6th Framework IST programme and is co-ordinated by FNB Netherlands (for recent publications cf. sources).

EUAIN brings together the different actors in the content creation and publishing industries around a common set of objectives relating to the provision of accessible information. Accessibility for print impaired people can be an increasingly integrated component of the document management and publishing process and should not be a specialised, additional service. Print impaired here refers to people who are blind, visually impaired or dyslexic. EUAIN takes the broadest definition of content creators and provides the support, tools and expertise to enable them to provide accessible information.

This article outlines the role of trusted intermediaries in accessible content processing workflows, giving examples of successful collaboration between content providers and specialist organisations. The regulatory challenges are also mentioned as are a number of technical and organisational considerations.

Technology and standards to serve groups with special needs are at hand

From a technical perspective, earlier problems relating to the digitisation of materials have been largely overcome and recent formats (such as XML, RDF, METS, MARC21 etc) provide a realistic basis for implementing the different aspects of this work. It is now possible to address the key concerns of content creators and providers and coherently to address issues such as: automation of document structuring, adherence to emerging standards, workflow support, digital rights management and secure distribution platforms.

For example, the recent Forrester Research report which foresaw publishers changing current business practices to match the internet's speed and convenience with the multichannel publishing model is now finding some practical application, which can offer greater consumer choice, variable presentations and delivery which is of crucial importance for those who require alternative formats. In Austria, it has been found that when publishers consider accessibility, their data can be re-used several times for multichannel publishing. As the lifetime of a book gets shorter and shorter, publishers frequently have to offer access to digital versions of that book and taking this into account when constructing the layout brings us much closer to real accessibility in the wider sense. Indeed, it has been the accessibility community that has in many ways pioneered new structures for digital content, as these developments are often borne of need. The recent EUAIN Workshop on Generating Structures examined these developments across Europe and the report is now available.

Similarly, emerging international and European standards provide an excellent basis for the creation of accessible information at a more fundamental level than has previously been possible. Whereas many earlier solutions have been at a 'workaround' level, with an accessibility component added at the end of the content creation process (if at all), it is now possible to see DAISY 3.0/NISO z39.86 as the de facto XML standard which can allow content creators significantly to enlarge their markets through the adoption of this inclusive format (cf. sources). Indeed, the navigational possibilities afforded by DAISY 3.0 are thus available to everyone, and not solely to those people who are print impaired.

At a European and national level, there now exists a clear desire on the part of publishers and associations of publishers to collaborate closely with experts in this area in order to provide truly accessible materials. Indeed, in several countries recent legislation has added an extra push to these concerns. This convergence at a technical, regulatory and political level means that the pieces of the jigsaw are now in place to make a significant breakthrough in the provision of accessible information within secure environments.

Trusted intermediaries and secure environments

Trusted intermediaries establish a personalised relationship between content holders and specialist organisations whereby publishers and agencies serving blind and partially sighted people work together in a secure and trusting environment to increase the quantity and timeliness of titles available in an accessible format. Within trusted intermediary frameworks, DRM is an enabler of controlled access. A number of different security methods are being developed or are already in use for making content available in this way.

As far as security is concerned, the higher the level the more likely publishers are to allow content to be made available in accessible digital formats. At present, the security systems used are simple, they use basic encryption technologies with key exchange mechanisms. The potential for the release of content is considerable – although there are few recorded instances of such occurring. Once decrypted, content is available to anyone, authorised or not. The ability to attach content to particular devices, or better to provide access only to authorised users, requires a level of DRM sophistication that is not yet generally in place in services catering to the needs of visually impaired people.

By way of illustration, in Belgium the national newspapers De Standaard and Het Nieuwsblad are offered in an electronic version (DiGiKrant) and a Braille paper version (BrailleKrant). This is achieved through means of a trusted intermediary. By placing a small specialist team within the newspaper publisher's offices, the alternative versions of the newspapers can be produced at the same time as the standard newsprint. Other solutions involve the news content being edited by external specialist organisations using online delivery mechanisms or delivery on CD-ROM.

In the Netherlands, an agreement was reached with the Dutch Publishers Association (Nederlands Uitgeversverbond) and the specialist organisation FNB whereby a small fee is paid for each title that is transformed into an accessible format. In addition, publishers have agreed to allow access to digital source files where feasible. This approach is an excellent example of an organisation (FNB) operating as a trusted intermediary and ensuring that the output materials are only given to registered end-users across secure distribution platforms.

In France, BrailleNet (cf. sources) has established contracts with more than 80 publishers and with an organisation managing the rights on behalf of publishers and this is the contractual basis of the Helene Server. Organisations that have been certified get an authorisation for a secured access to source files. The server Hélène contains both literary and school books in French and publishers who have contracted with BrailleNet provide the files. In the UK, RNIB has good working relations with several publishers and has been developing the *trusted intermediary* concept, and one collaborator is one of the world's largest publishers.

Challenges ahead

DRM solutions prevent content from being accessed by any person that has not been authorised to do so. This protection can happen at different levels, ranging from opening and reading the document to copying and transforming it. Agencies producing materials in alternative formats to serve persons with disabilities need to access content in order to transform it into formats that are suitable for those who cannot read it in the way it has been originally produced. Naturally these considerations also apply within mainstream publishing workflows where accessibility can also be incorporated.

The European Directive on Copyright (2001/29/EC) expresses the right to access content without any technological protection measures when the exemption for persons with disabilities has been adopted by the national legislation but at the time of writing this EC Directive has been implemented in a variety of different ways. WIPO has also recently included similar exemptions as a recommendation to those countries in the process of setting up copyright legislation. A further problem related with copyright and intellectual property rights has to do with transnational interchange of materials. Some copyright legislations allow only for the use and transformation of documents within the boundaries of the country where it has been originally produced, which automatically eliminates the possibility of making it available to persons with the same needs, sharing sometimes the same language, in a different part of the world. The World Blind Union (WBU), IFLA Libraries for the Blind Section and WIPO have recently initiated a survey to examine the barriers to international transfer of accessible materials in order to draw conclusions and to make recommendations on any need for changes to national laws or international treaties received the support of many countries.

Alongside these regulatory challenges, a number of technical and organisational challenges are also relevant. In this sense we must see accessibility itself as a process and not a product, a characteristic shared by DRM systems. When considering notions of access, four further issues are noteworthy:

- access to structured digital formats

Currently there are many digital formats that are inaccessible to persons with disabilities even through adaptive technology. Those formats that are based mainly on images that are not described properly are very difficult to access. Very little attention is paid to structuring information through tagging.

Documents that use tags for describing the different elements in their structure (like XHTML or XML) are of great use for those agencies producing accessible materials. Emerging multimedia formats offer opportunities to embrace accessibility issues, especially when they're based in highly structured formats and MPEG is particularly important in this respect. Within MPEG modelling environments, interfacing between Accessibility and DRM objects is highly feasible.

- access when and where it is needed

When information has to undergo complicated and costly adaptation post-processes before becoming truly accessible, the delay in getting access to that information can be excessive. Access to information in digital formats allows for easy and fast distribution to anybody at any time. The distribution of source files in a format that can be easily translated into other accessible formats allows also for customization of the information before being finally delivered to the user in the required format. Just-in-time distribution (as opposed to Just-in-case storage where everything is digitised) would actually help in making information accessible in a more efficient way.

- access to source materials

Accessing materials at source prevents agencies from spending resources on re-digitising final products. This saves time and resources in giving services to those who cannot read printed materials. If that source material is provided in a format that is already prepared for further transformation and in an agreed standard form, the time and resources saved will be even bigger. However, content providers are usually reluctant to provide publishers of materials in alternative formats with their digital masters. Fear of piracy and the evident ease in which this happens in the digital world are usually the main reasons given by publishers. As noted above, agreements with publishers in which these agencies are seen as *trusted intermediaries* seem to be the most viable solution to this situation.

- access to consistent content

Publishers of accessible materials are aware of the importance of creating consistent content. Their function is to make content accessible, the same content that is available for persons without disabilities, without altering it, without adding to or taking any information away from the original, except where extra information is needed to describe what cannot be made accessible otherwise (pictures, charts, graphics, etc.). It is important for content providers (e.g. medicine labelling) that correct and approved information is used and nothing is lost during the transformation process. Using the information provided directly by the original publisher helps in guaranteeing this. It is also important for the impaired user that no information is lost, so that the content they can access is exactly the same as that originally published. Greater co-operation is required between EU countries to avoid duplication of effort and expense as separate national practices prevent from interchanging materials that are already available in other countries.

Bottom line

It can be seen that the choice of appropriate technical protection measures for making content accessible is not straightforward and involves different considerations. The *trusted intermediary* approach has provided concrete examples of successful collaboration. Where appropriate, light DRM solutions have been applied. Further research is required to examine accessibility in the wider sense and to examine the requirements for modelling accessibility and DRM within emerging multimedia environments.

Sources

- Crombie, D (ed) (2005): Generating structures , EUAIN Consortium, Amsterdam; http://www.euain.org/modules/wfsection/article.php?articleid=161
- Crombie, David; Lenoir, Roger; McKenzie, Neil (2005): Towards accessible content management systems, ELPUB2005, Leuven Belgium, see http://anderslezen.nl
- DAISY Consortium: http://www.daisy.org

- du Bourguet, Guillaume; Guillon, Benoit; Burger, Dominique (2003): Helene: a collaborative server to create and securely deliver documents for the blind. Proceedings AAATE 2003, see http://serveur-helene.org
- European Accessible Information Network (EUAIN): http://www.euain.org
- Forrester Research (2000): Books Unbound, http://www.forrester.com/ER/Press/Release/0,1769,470,FF.html
- Garnett, N., Mann, D. & White, M., (eds) (2005): Accessing & protecting content, EUAIN Consortium, FNB, Amsterdam
- Standing Committee on Copyrights of WIPO, 21-23 November 2005

About the authors: The authors co-ordinate the EUAIN network for FNB (NL) and RNIB (UK). *David Crombie* is head of the FNB International Projects department in Amsterdam, alongside researchers *Roger Lenoir* and *Neil McKenzie*. The team has been active in many EC funded research projects over the last ten years, in particular relating to *eInclusion*, Cultural Heritage and Digital Libraries. *David Mann* is a Campaigns Officer for RNIB, and has focussed in particular on copyright issues and on the Right to Read campaign. As well as working at national level, he has been active in developing links with the World Intellectual Property Organisation (WIPO) and the International Publishers Association. Contact: nmackenzie@fnb.nl

Status: first posted 26/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=169

Digital rights management and accessibility

By: Zoltán Nagy, Speech Technology Ltd, Budapest, Hungary

Abstract: The article addresses accessibility issues for blind and visually impaired consumers. Technical tools like OCR, text to speech engines, and screen readers are introduced. Limitations of these tools as well as new promising approaches are discussed. Finally attention is drawn to the problems disabled people face when using websites, software, and mobile phones.

Keywords: technical analysis - accessibility, consumer expectations, disabled, talking books

Introduction

An everyday story

On an average summer day Mr. Smith, an average visually impaired man, goes into an average library to try to read an average monthly. He goes to a computer and realizes there is no screen reader installed – a screen reader is a software application that attempts to identify and interpret what is being displayed on the screen. No problem he thinks, he goes home and takes his notebook with a screen reader to the library. However the employees of the library refuse this solution suspecting Mr. Smith might be going to launch a publishing company. So he asks the librarians to scan the article he is interested in so that he can read it out with his own computer at home. This does not work either, because the librarians are not allowed to let anything leave the institution in electronic form. Eventually Mr. Smith goes back home with a single copy of the article in print. This situation is neither satisfying nor transparent for both actors: the visually disabled and the librarians.

Visually impaired persons are consumers like you and me

In the European Union there are more than 10 million people who have significant sight loss and are not likely to be able to read printed news. Since average life expectancy is continuously rising, more and more people have impaired sight. These people do not identify themselves as blind or partially sighted, but they are only able to read published materials by using alternative methods.

We have no exact statistical figure about the number of people suffering from dyslexia or

about the state of their disability, but according to experts about 4% of the population is severely dyslexic. A further 6% have mild to moderate problems.

Naturally some aspects of the lives of blind people are significantly different from average people, but considering the consumption of (digital) contents they are not different at all. They listen to radio and television, they usually have CD and/or DVD players and they buy films. They are up-to-date with regard to movies, celebrities and series like anybody else. These offerings are essential for them to be full members of society.

In this article we try to give an overview of the technologies which assist the visually impaired in being consumers and users of content, and the accessibility problems they face. It also outlines a solution to some of the problems.

Technology: TTS and screen readers

To use a computer a blind person needs a text to speech engine (TTS) that can read texts out. TTS is responsible for speaking but not what to speak. Under Windows operating systems TTS engines usually support Ms Speech API – which is the standard way to create speaking enabled applications.

A screen reader is a special application which can narrate applications, or screen, or system and keyboard events. It echoes keypresses, appearance of windows and message boxes (even system bubbles of XP). Screen readers do not use OCR techniques. Optical character recognition involves computer software designed to translate images of typewritten text (usually captured by a scanner) into machine-editable text. Screen reader applications are based on special programming techniques, so called hooking, and a lot of heuristics and scripts. Usually it contains a special display driver, which tries to catch/capture the text printing function calls. This application interprets the screen for the blind and speaks out every message by a TTS engine.

There is a small group of applications which are developed for the blind: usually special blind games or learning environments or web browsers. Such software can be used by the blind without any screen reader application. The user interface of these applications is designed for the special requirements of blind users.

Limits and problems of screen readers

The first screen readers applied hooking mechanism (under Windows), but as time went on they became more and more complicated and it got more and more difficult to get textual information off the screen. Some applications even deliberately prevented other applications from getting text from that application. A wide known example is the Adobe Acrobat Reader in its earlier versions.

Furthermore, screen reader software is unable to read textual documents appearing in the windows of that application. This phenomenon is typical for applications which have their own text drawing function. To solve this problem companies like Adobe offer accessibility packs on their websites. After installing such a pack it is possible to read the document aloud from the menu. Later versions (6.0 and later) of Adobe Acrobat Reader have incorporated that function directly. The functionality however is quite poor, because only individual pages or full documents can be read aloud. An up-to-date screen reader software should be able to read out text parts of different sizes (page, paragraph, sentence, word and letters too)!

Microsoft specified the IAccessibility interface as a standard way to give information to screen readers. Unfortunately, this interface is supported by only few applications, because its implementation would mean a lot of "unnecessary" additional effort.

As a matter of piquancy, different by-passes - like the one used by Adobe Acrobat Reader - do not guarantee to prevent getting content. A professional software developer can develop a fake TTS with just 15 minutes' work, which instead of reading the text aloud collects it in a file. This manoeuvre can be performed with the IAccessibility interface too. However, as the user interface does not allow reading complete documents aloud contiguously but just in small pieces, this type of attack is made difficult here

From simple voice books to DAISY books

A printed book is available to a blind person by scanning, then transforming the text with the help of OCR software into digital text and reading it out by a screen reader. This long and complicated task can be performed by a blind person after practicing it for a while provided he or she has the needed equipment. We can imagine what an overhead of work this means for each blind person to scan the same book. In practice, blind people share books scanned and transformed into speech, and blind peoples' organisations collect these materials, tolerated by copyright owners. Some countries allow copying books in that way for people with disabilities provided it is not for profit. Copyright owners tolerate this. However, publishers are more and more afraid, and not without ground, that books digitised in that way can easily be shared via file sharing applications. To digitise a book is hard work. Average users will not start to scan and recognise (by OCR) a hundred-page long book, but if he or she has ready access, that's quite a different story.

In the beginning voice books were recordings available on different media. Then, with the spread of computers they appeared in more and more sophisticated forms. The length of audio files on a single CD was increased by compression. Hybrid talking books also appeared which contained the book in text and in voice form as well making the content capable for key word searching. Talking books are not only for people with disabilities. The value of a literary work can be increased if it is performed by a well know actor.

In this context the DAISY standard is very important. The DAISY Consortium was formed in May 1996 by talking book libraries to lead the worldwide transition from analogue to digital talking books. DAISY denotes the Digital Accessible Information SYstem which is the standard, when we talk about books made for visually impaired. This is a very widespread format used all over the world from the USA to Japan. The secret of the success of DAISY is that it uses a simple open format. Not only player software and devices but various types of DAISY editors are available. Many of them can be used by the blind, so organisations of the visually impaired can make their own talking books. DAISY digital talking books contain the text in XML format plus the high quality voice record synchronised with the text. DAISY books are distributed on CD-ROMs and there are many portable players. DAISY does not make possible either the encryption of information or the identification of users, which is a limitation in terms of DRM, because it relies on these two components. For more details see the DAISY standard; cf. sources). However, many books are published in that form worldwide not only for people with disabilities.

An innovative solution from Hungary

There are solutions which aim to take everybodys' interests into consideration. "Világhalló" is a Hungarian service supported by Hungarian publishers which started in 1999. Világhalló is an integrated on-line service which forwards available texts as a combined text and voice flow to the user (as a text radio) using special voice-text synchronised protocol (wow) developed specially for this purpose. By the way, "Világhalló" is a play on words which converts the Hungarian name of the Internet to "World Listener". Copyrighted content is stored on a secure server and a client program downloads the voice. This solution has an advantage regarding copyright, because the text alone is not accessible by the user. This is in line with the publishers' requirements.

"Világhalló" deals with stored text, irrespective of its genuine format (HTML, ZIPHTML, TXT, ZIPTXT, MSWORD, RTF, XML, SGML) and transforms it into a format for best reading aloud. The software adds to the text informative, structural annotations concerning the reading aloud (like sentence, paragraph, strophe, chapter, etc. or foreign word pronunciation even in inflected form).

This system is mostly used by the blind, since it is not really suitable for everyday people. Publishers make some of their copyrighted products available to gain experience. In the early phases of Világhalló it had no users at all, because accessing the content needed continuous broadband Internet ac-

cess, which meant high cost, especially for the blind. During the last six years, the service has overcome the first difficulties, and now it has 16.000 users. What is more, it has managed to get the full trust of publishers and within a few weeks works published by Magvető, one of the leading Hungarian publishing companies, will become available on Világhalló.

Accessibility issues beyond books

Problems using websites

Questions connected to persons with disabilities are not always technological. Many publicly available free contents are not accessible for visually impaired people, because the content is visually organised in such a way that without seeing it, the text turns into an unembraceable continuum. An excellent example for this is an average news portal. The structure of pages targets the majority of visitors. To make such a portal readable for visually impaired people we have to make many simplifications. Fortunately, contents are stored in databases by up-to-date portal engines so a blind friendly version can easily be produced simultaneously with the normal appearance. Governments could motivate companies to work on these developments by subsidised tenders. In the ideal case, this would even provide work for people with disabilities to be involved not only in testing but in development too.

Problems using software

Access to content is difficult for the visually impaired, but so is the use of software. I do not mean here sophisticated programs like a video editor, but the most essential programs. Many software user interfaces use exotic or mouse optimised controls which can not be handled by screen readers. That would not mean a problem itself if the impaired could choose an alternative solution, another software. The trouble however is, that this phenomena often occurs even in developments targeting visually impaired people! Although there is an ergonomic standard for such applications, many developments don't take it into account. This situation could be avoided if someone really concerned were to work in a developer team, and if the opinions of people concerned were collected in the design phase.

Problems using high-tech gadgets

Most music players use LCD displays to display textual information. This is totally unusable for a visually impaired person. However, many blind people use such equipment, simply memorising the menus and the order of the buttons. Many of the blind, using the same method, are able to even send SMS. The use of mobile phones is one of the challenges facing the vision-impaired. Mobile phones are designed primarily on visual concepts, without considering the needs of the blind or partially sighted. There are some screen reader solutions for mobile phones that allow access to most of the functionality of the device. These are designed to work with the Symbian-based operating system (mostly business class Nokia and some Ericsson, Samsung, Panasonic and Siemens phones). These products allow access to all of the phone's applications, including third-party applications.

Bottom line

The biggest accessibility problem today is that publishers and copyright owners are not, or not really, interested in serving the blind or people suffering from dyslexia. If there were a standard system which ensured copy protection and made content available in digital form, the visually impaired would become a valuable market for publishers.

Sources:

- American Library Association (2005): Digital Rights Management and Accessibility; http://www.ala.org/ala/washoff/oitp/emailtutorials/accessibilitya/10.htm
- Anderson, Ross (2003): Trusted Computing Frequently Asked Questions (Version 1.1 (August 2003); http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Clark, Joe (2003): Accessibility implications of digital rights management; http://www.joeclark.org/access/resources/DRM.html

- DAISY: http://www.daisy.org (The DAISY Consortium was formed in May, 1996 by talking book libraries to lead the worldwide transition from analogue to Digital Talking Books. DAISY denotes the Digital Accessible Information System).
- Kerscher, George; Kawamura, Hiroshi (2001): DRM for persons who are blind AND/OR print disabled; http://www.w3.org/2000/12/drm-ws/pp/daisy.html
- Világhalló portal – Online Reading System: http://www.vilaghallo.hu/english.html

About the author: Zoltán Nagy is the Head of Development at Speech Technology Ltd. which develops speech processing solutions and has taken part in many projects aiming visually impaired users. For more information see: http://www.speect.com

Status: first posted 26/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=168

DRM interoperability and reusability through a generic software architecture

By: Sam Michiels, Koen Buyens, Kristof Verslype, Wouter Joosen and Bart De Decker,
Dept. of Computer Science, K.U.Leuven, Leuven, Belgium

Abstract: The domain of digital rights management (DRM) is currently lacking a generic software architecture that supports interoperability between and reuse of specific DRM technologies. This lack of architectural support is a serious drawback in light of the rapid evolution of a complex domain like DRM. It is highly unlikely that a single DRM technology will be able to support the diversity of devices, users, and media, not to mention the wide variety of requirements concerning security, flexibility, and efficiency.

Keywords: technical analysis – DRMS, DRMS research, interoperability, software architectures

Challenges to DRM development

Systems that provide digital rights management (DRM) are highly complex and extensive: DRM technologies must support a diversity of devices, users, platforms, and media, and a wide variety of system requirements concerning security, flexibility, and manageability. This complexity and extensiveness poses three major challenges to DRM development, which provide the context of this article: fragmentation of individual solutions, limited reuse of and interoperability between DRM systems, and lack of a DRM software architecture that supports and guides the design and implementation of DRM systems and their applications.

- The first challenge relates to the fact that state-of-the-art DRM technologies are often ad-hoc, which leads to fragmented DRM solutions (e.g. for music, for pictures, or for digital TV) and makes it very difficult to complete the complex and extensive DRM picture.
- The second challenge, limited reuse and interoperability, is partly caused by in-house developed solutions that are incompatible with similar systems produced by other parties. Currently, for instance, an access service implemented by Apple cannot easily be reused in a Microsoft DRM system, even if both parties would like to do so. Although various DRM developers have produced "vertically integrated" designs in which their particular set of components are specifically conceived to collaborate, their solutions are unable to interoperate with components from other groups. Given the complexity and extensiveness of DRM, interoperability between specific DRM services is crucial to allow (small scale) projects to contribute to the development of particular DRM services (Jamkhedkar and Heileman, 2004).
- The third challenge, lack of a DRM software architecture, is typical for complex software systems in evolution, and pro-

viding a software architecture is often a sign of growing maturity of the application domain. A software architecture can be seen as a generic structure that identifies the main service components and shows how they can interact. Having available such generic structure helps to evolve towards a complete set of interoperable DRM service components.

The challenges of integrating independent service components are well-recognized and are being addressed in other application domains than DRM, such as network communication, web services, or graphical user interfaces. The Internet architecture, for instance, convincingly demonstrates how a properly chosen software architecture can shape the evolution of a complex system across vast changes in technology, scale, and usage. The power of the Internet lies not so much in the elegance or efficiency of its individual components, but in the overall ability to encompass tremendous growth in scale and diversity as usage and technology continue to evolve.

A layered DRM architecture as solution

This article describes an academic study that argues for a layered DRM architecture that supports DRM developers in producing complete and interoperable systems (Michiels et al., 2005). The architecture is approached from both a functional and a security perspective. The functional perspective zooms in on the top layers, closest to the applications using the architecture. The security perspective focuses on the bottom layers, which offer cryptographic primitives to enforce digital rights. In other words, the cryptographic primitives at the bottom layers lay the foundation for the upper layers to build upon. Finally, the proposed architecture is validated by matching it to state-of-the-art DRM technologies.

Our study presents a layered architecture and identifies the key DRM services of each layer. The main contribution of this study is that it presents a next step towards a software architecture that supports reuse and cooperation of multiple domain-specific DRM technologies and standards. It is our belief that this architecture lays the foundation for addressing the above-mentioned challenges of fragmentation, reusability and interoperability, and guides developers of DRM software systems and applications in the right direction.

The proposed architecture in a nutshell

The study presents the main system requirements from three application viewpoints: the content consumer's, the content producer's, and the content publisher's. In addition, it identifies for each viewpoint the core functional services that are needed in a complete DRM system to provide this application-level functionality. In this way, seven key DRM services have been identified (see Figure 1): the Content Service (e.g. search for content), the License Service (e.g. issue licenses), the Access Service (e.g. authenticate consumers), the Tracking Service (e.g. produce usage statistics), the Payment Service (e.g. billing), the Import Service (e.g. submit content to the DRM system), and the Identification Service (e.g. reveal abusers). Next to functional services, the study identifies the hot spots in this architecture that require specific security services (such as authentication, confidentiality, and anonymity), and the cryptographic primitives needed to implement them (e.g. watermarks, digital signatures, certificates, and encryption). Remark that a single security service can be implemented by multiple cryptographic primitives depending on the requirements. For example, user authentication can be implemented by using digital signatures; yet, if user anonymity is required as well, other techniques such as zero-knowledge proofs must be used instead. The functional and security services are combined and presented in an architectural overview as shown in Figure 1. The model consists of a distributed view and perspectives from the side of the consumer, the producer, and the publisher, a layered architecture for each party, and identification of components in each layer.

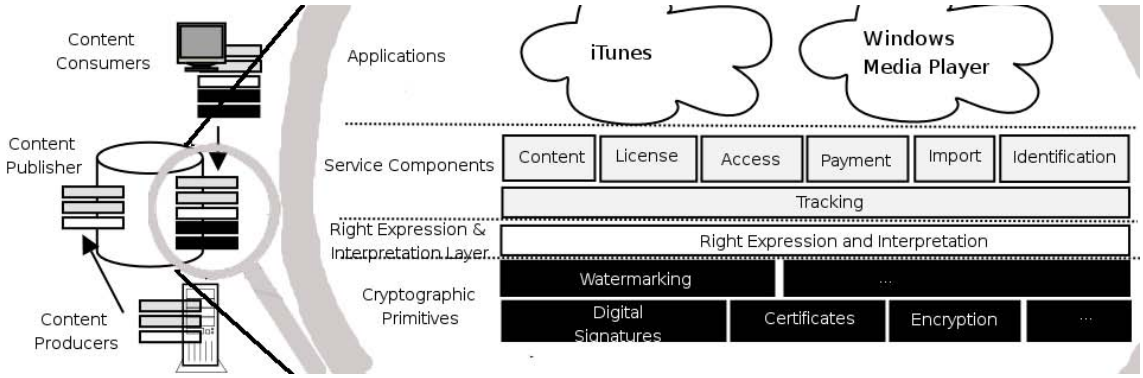

Figure 1: A distributed view on an architecture for DRM with a content consumer, producer, and publisher. The figure zooms in on the layered architecture of the publisher

Validation of the approach

By way of validation of the proposed approach, the study maps state-of-the-art DRM technologies onto the architecture and discusses how it supports the three main challenges formulated earlier. The validation is based on six DRM technologies on which technical information was publicly available: Windows Media DRM, Lightweight DRM, EMMS, Helix DRM, Aegis DRM, and the OMA specification.

Table 1: Overview of provided services of state-of-the-art DRM technologies.

DRM tech/ Service	Content	License	Access	Tracking	Payment	Import	Identification
WMDRM	X	X	-	X	-	X	-
LWDRM	X	-	X	-	X	-	-
EMMS	X	X	X	X	X	X	-
Helix	X	X	X	X	-	-	-
Aegis	-	X	X	X	-	-	-
OMA	X	X	X	-	X	-	-

As the overview in Table 1 shows, some services are provided almost uniformly by all technologies, while others are only offered sporadically. The Content and License Services are almost always implemented, which seems nothing but normal for such key services. Services for accessing, tracking, paying and importing are provided in approximately 50% of the cases, while the Identification Service is not implemented by any of the studied DRM techniques, at least not to our knowledge.

When relating these results with the three main DRM challenges presented in the introduction (completeness, interoperability, and software architecture support) we can draw the following conclusions.

- First of all, the fact that so many different DRM technologies implement the same or similar services confirms our claim that we need an architecture that promotes reuse of and interoperation between individual service components.
- Secondly, the study shows that the services with the highest benefit from reuse and interoperation are the Content and License Service. All DRM technologies that need these services would benefit from a reusable implementation.

- Thirdly, since judging from the study different DRM technologies implement different sets of services, trying to standardize 'the' DRM technology seems less efficient than focusing on particular services these technologies are composed of.

DRM architecture and Internet architecture compared

This brings us back to the analogy with the Internet architecture, which clearly identifies service responsibilities and a common platform that can support a wide variety of networking services. This architecture proves that a complete solution can be offered by a single platform if it allows reusable services to be plugged in, without trying to provide a single overall standard implementation. In other words, although service implementations may vary (for example, the access service implementation on a mobile phone will clearly be totally different from a version for a desktop computer), the architecture in which a service component is embedded and the interfaces it provides to other service is always the same. Until today, many different companies and organizations extend the TCP/IP architecture with protocols for quality-of-service, wireless communication, media streaming, or security. If we are to provide complete DRM solutions, following the Internet approach seems to be a good idea.

However, we should be aware that the Internet approach cannot be adopted as such in the domain of DRM. Although the idea of using a layered architecture for DRM solutions looks very promising, we have to be aware that the match between TCP/IP and DRM is not complete for two reasons. First of all, the DRM architecture does not completely adhere to a layered structure. This is especially true when looking at the architecture from the perspective of adaptability and manageability, two crucial quality attributes for DRM systems, which often have to be tuned to various business policies or local legislations. Such concerns can turn the main advantage of layering, i.e. virtualization of lower layer details, into a major disadvantage. This situation occurs, for instance, when lower layers do not behave exactly as required by upper layers or applications. In this case, applications should be able to fine-tune the underlying system by injecting specific policies. This is a generic problem that has already been explored in other application domains than DRM.

The second reason to be careful when comparing TCP/IP and DRM is that the architecture of the latter will not always be symmetric: while a TCP/IP client runs exactly the same protocols as the server, this is not necessarily the case for DRM systems. The right expression layer, for instance, will probably be fully implemented on the publisher's side to allow for content producers to associate with their content a wide variety of business policies. Yet, from a content consumer's perspective, this layer will typically be minimally implemented to prevent clients from tampering with business policies. The same is true for rights enforcement technologies such as watermarking, digital signatures, or certificates.

DRM Architecture and DMP compared

The Digital Media Project (DMP web site, 2005) proposes a similar approach to increase interoperability of DRM services. It defines users (e.g. consumers, producers, or publishers) as entities that perform so-called *primitive functions,* which represent the underlying DRM services that handle digital content. The primitive functions can be related to the functionality of the service components (e.g. revoke user), the rights expression and interpretation layer (e.g. represent rights expression), or the security components (e.g. represent key). The DRM architecture we have presented structures the domain by locating the set of primitive functions (components) in three layers: the service components layer, the rights expression and interpretation layer, and the security layer. Both approaches focus on interoperability by providing functions (components) with well-defined responsibilities.

Bottom Line

The presented model has confirmed the potential benefits of applying software architectures to inventory, analyze, and discuss research in this field, and has proven to be use-

ful to set the agenda for the future. If DRM is not to end as the umpteenth flash in the data protection pan, it may be high time to put software architecture design at the top of its research agenda. In our opinion, the next steps to be taken in this research field are (1) to refine the interaction interfaces of the identified service components, and (2) to apply and validate the proposed architecture in a case study to reveal additional issues driven by non-functional requirements (e.g. efficiency of content distribution, content personalization, or context awareness).

Sources

- The Digital Media Project (DMP) web site (2005): http://www.dmpf.org
- Jamkhedkar, Pramod; Heileman, Gregory (2004): DRM as a Layered System. In: Feigenbaum, Joan; Sander, Thomas; Yung, Moti (Eds.) Proceedings of the 4th ACM workshop on Digital Rights Management (DRM'04), Washington, DC, USA. ACM Press, pp. 11–21.
- Michiels, Sam; Verslype, Kristof; Joosen, Wouter; De Decker, Bart (2005): Towards a Software Architecture for DRM. In: Safavi-Naini, Rei; Yung, Moti, (Eds.): Proceedings of the 5th ACM Workshop on Digital Rights Management (DRM'05), Alexandria, VA, USA. ACM Press, pp. 65-74.

Acknowledgements: This article is a summary of (Michiels et al., 2005) and presents a study which brings us one step closer to a generic software architecture for DRM. Research for this article is part of the E-PAPER project, funded by the Interdisciplinary institute for BroadBand Technology (IBBT). The project is being carried out in collaboration with a consortium of companies: Philips, De Tijd, Belgacom, Hypervision and I-Merge. The authors are very grateful to Ann Heylighen for her valuable comments and for proof reading the text.

About the authors: *Sam Michiels* is a postdoc researcher at the Computer Science Department of the K.U.Leuven. He received his Ph.D. in computer science in 2003. His main interests include software technology and network middleware. *Koen Buyens* is a researcher in the Computer Science Department of the K.U.Leuven. His main interests include secure development of applications and middleware. *Kristof Verslype* is a Ph.D. student at the Computer Science Department of the K.U.Leuven. His main interests include secure software and anonymity. *Wouter Joosen* is professor at the computer science department of the K.U.Leuven. His research interests include software architectures for distributed systems, aspect-oriented and component-based software development, and secure software. He received his PhD in computer science from K.U. Leuven. *Bart De Decker* is professor at the Computer Science Department of the K.U.Leuven. He received his PhD in computer science from K.U. Leuven. His research interests include secure software, privacy, and anonymity.

Contact: sam.michiels@cs.kuleuven.be / bart.dedecker@cs.kuleuven.be / koen.buyens@cs.kuleuven.be / kristof.verslype@cs.kuleuven.be / wouter.joosen@cs.kuleuven.be

Status: first posted 25/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=167

DRM for digital broadcasting in Japan

By: Kiyohiko Ishikawa, NHK (Japan Broadcasting Corporation), Tokyo, Japan

Abstract: Digital broadcasting has already been operational in Japan for years. All Japanese digital broadcasting is scrambled, but free to air, except for a few Pay TV channels. All contents and copyrights are protected by CAS (Conditional Access Systems). This article describes the current state of these digital broadcasting systems using CAS. It also shows that the realization of content protection and management in broadcasting requires a mechanism to execute some form of enforcement in the STB (Set Top Box).

Keywords: technical analysis – conditional access, digital broadcasting, digital TV, DRMS - Japan

Introduction

In Japan digital broadcasting has already been launched. BS (Broadcasting Satellite) started in 2000 and terrestrial digital broadcasting in 2003. All Japanese digital broadcasting is scrambled, but free to air, except for a few Pay TV channels. Content and copyright are protected by CAS. The function of CAS is implemented on a B-CAS card which is an IC card. The function of CAS is described later. Each STB has a particular B-CAS card. The B-CAS card is managed by BS Conditional Access Systems Co., Ltd. (cf. sources). Two types of B-CAS card exist: the red and the blue card. A red card is commonly used for BS, 110 degree CS, and terrestrial broadcasting. 110 degree CS is an independent pay TV service. A blue card is only for terrestrial broadcasting. If no B-CAS card is inserted in a STB, that STB cannot descramble scrambled content. The specification of these digital broadcasting depend on ARIB (Association of Radio Industries and Businesses standards; cf. sources).

The objectives of ARIB are to conduct investigation, research & development and consultation of utilization of radio waves from the view of developing radio industries, and to promote realization and popularization of new radio systems in the field of telecommunications and broadcasting. An important task of ARIB is the establishment of technical standards for radio systems in the field of telecommunications and broadcasting. Overall, ARIB aims at the promotion of public welfare.

The current state of digital broadcasting

10 million STBs were in use for BS digital in September 2005. When terrestrial digital broadcasting started in the Tokyo, Osaka and Nagoya areas on December 1, 2003, the number of terrestrial digital STBs was about 300.000. In the meanwhile more than 5 million terrestrial digital STBs are being used.

There are eight TV broadcasters including data broadcasting, four data broadcasters and five radio broadcasters in BS digital broadcasting. HDTV (high definition) and SDTV (standard definition) services are respectively seven and two channels.

The digital terrestrial TV broadcasts have also the high picture and sound quality of digital high definition (Hi-Vision) and attractive interactive features. Data broadcasting in Japanese characters provides information tailored to each locality. The digital terrestrial broadcasts are received by UHF antenna. The reception of sound and images is clear even on the STBs installed in moving trains, buses etc. A service for simple moving images, data and radio reception on mobile terminals etc. is also anticipated.

There are NHK and five commercial broadcasters which are major network TV companies and two local broadcasters in Tokyo area. Thus Japanese digital broadcasting which uses CAS is successfully spreading.

DRM in digital broadcasting systems

Japanese broadcasters encrypt content for copy protection, regional control of viewing, pay TV charging, etc. The encrypted content is transmitted to the subscriber's STB, which

decrypts the encrypted content. Since each STB has a decryption key in its B-CAS card, it can decrypt content. It is possible to distribute different decryption keys to STBs in different areas, and thereby enable regional control of viewing. For pay TV, only the subscribers who sign a contract with a broadcaster can get a decryption key, and in this way broadcasters control access to the content.

The DRM standardized in Japan employs a three-step encryption system. The subscriber reveals his/her identity to a broadcaster and gets a B-CAS card. The B-CAS card is used as a tamper resistant module. Each B-CAS card has a unique master key, *Km*, that is stored in the tamper-resistant part of the card. *Km* is shared with broadcasters and is used to encrypt personal contract information when the broadcasters transmit information to a subscriber's STB. *Figure 1* shows a block diagram of the conventional DRM system for the Japanese digital broadcasting system.

In the broadcasting station, contents are scrambled with a scramble key, *Ks*. The scramble key is encrypted with a work key, *Kw*, and the work key is encrypted with a master key, *Km*. After that, the encrypted contents and keys are multiplexed and transmitted to the subscribers' STBs. This procedure is called a three-step encryption.

The STB receives the encrypted contents and keys and de-multiplexes the encrypted content, scramble and work keys. It sends the encrypted session and work keys to the B-CAS card, which has been put in the STB. The B-CAS card decrypts the work key with the master key it holds, after which it decrypts the session key with the decrypted work key. The STB then gets the session key from the B-CAS card and decrypts the encrypted contents. In this way, subscribers can watch/listen to the content.

Of these three keys, *Ks* is changed every few seconds when the contents are encrypted to ensure security. *Kw* is the key that authorized subscribers get when they make a contract with a broadcaster. This key is updated with every contract. *Km* is a private key, and it is used to encrypt each contract when the contract information is sent to the B-CAS card. If broadcasters were to transmit *Kw* to all subscribers, they would need to encrypt and broadcast all the *Kw*s. Such a broadcast would require a capacity in proportion to the number of subscribers, and thus it would impose a large load on the transmission channel. To decrease the load, *Kw* is broadcast only when it is to be updated. With these three keys and three-steps encryption, broadcasters can protect the copyrights of their contents. Moreover, to control the viewing region, as *Kw* is encrypted with *Km* and transmitted, broadcasters have to know each subscriber's (B-CAS card's) location.

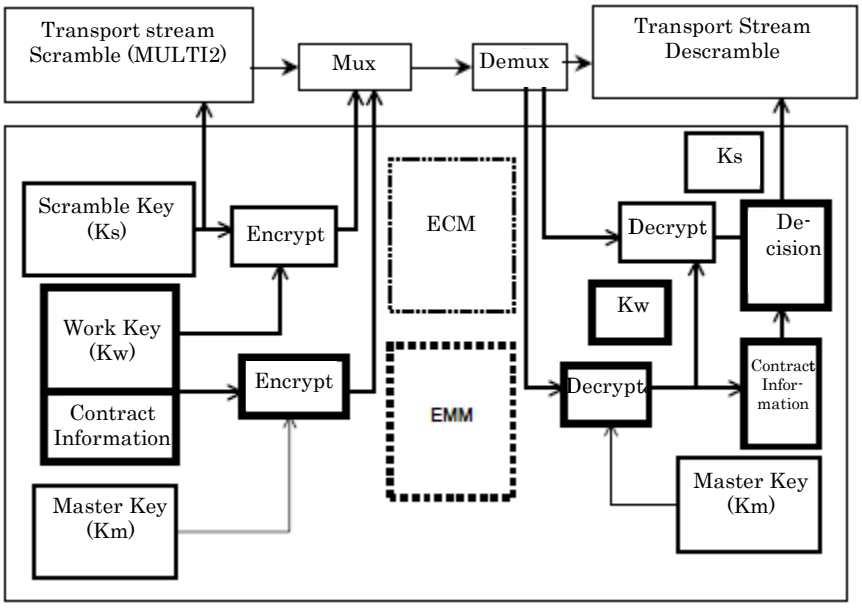

Figure 1: Conventional DRM system

Broadcasters then transmit the encrypted *Kw* to the subscribers that are in the region where the program is allowed to be viewed. This system can control viewing region. For pay TV, *Kw* is transmitted to subscribers who pay for programs or for channels. This system can realize pay TV.

Broadcasting System based on home servers

Broadcasting System based on home servers is a next-generation broadcasting system that utilizes a PDR (personal digital recorder) which is an STB with a large capacity storage, and it is now in the process of being standardized. It employs a four-step encryption. *Figure 2* shows the block diagram of the proposed DRM for Broadcasting Systems based on Home Servers. It is assumed that the transmitted contents will be stored in the receiver, and it is required that conventional broadcasting services can be also received. Hence, the proposed DRM can be constructed by adding a new encryption key to the conventional DRM. The new key is called "content key" (*Kc*), and it is used to encrypt the session key when the content is stored in the PDR. *Kc* may be unique for each content. But actually *Kc* does not have to be unique for each content. It depends on the broadcaster.

Moreover, another new key is introduced. It is called "group key" (*Km'*). But *Km'* will be called domain key with use home network. STBs with the same Km' belong to the same domain. STBs in the same domain are able to use each other's stored contents because they have the same encryption key *Km'*.

Km' is set in the CAS card. As shown in *Figure 2*, *Kc* is encrypted with *Km'* and stored in the STB. *Ks* is also encrypted by *Kc*. Since each STB's *Km'* is different from any other *Km'*s belonging to other CAS cards, once *Kc* is encrypted with a *Km'* of a specific CAS card, it is impossible to decrypt the correct *Ks* by using a *Km'* of another CAS card. Hence, it is impossible to decrypt correctly content from the stored encrypted content that is moved or copied from another subscriber's STB.

Furthermore, Broadcasting System based on Home Servers uses Rights Management and Protection Information (RMPI). RMPI includes copy control information, playback control information, region information, output device control information, etc. When the content is used, the PDR checks the RMPI and controls its processes accordingly.

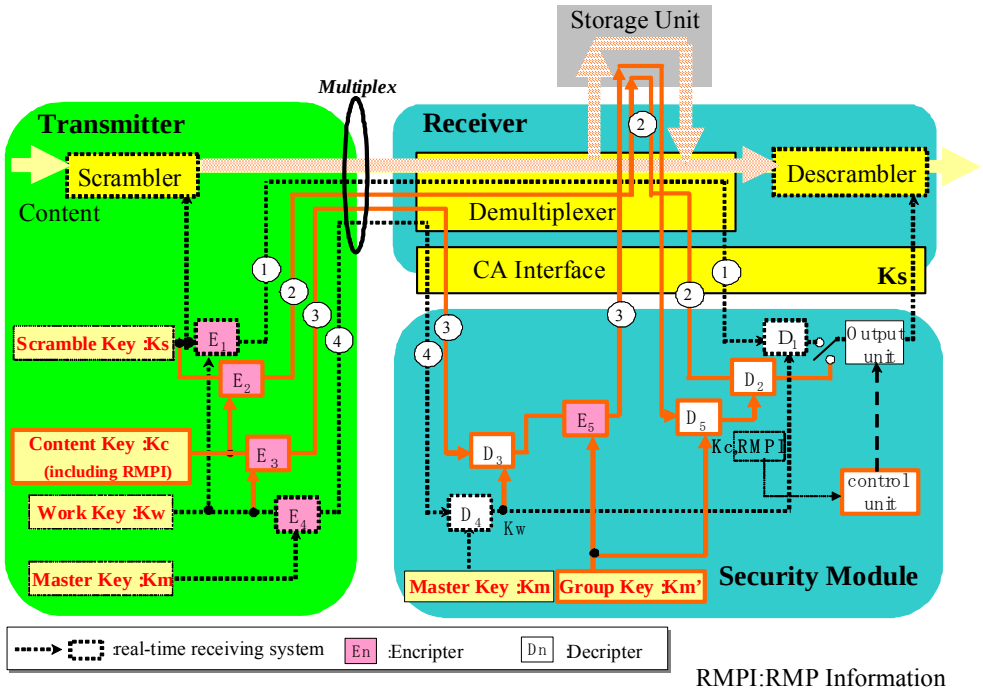

Figure 2: DRM for Broadcasting System based on Home Servers

Content copy control

The realization of content protection and management in broadcasting requires a mechanism to execute some form of enforcement in a STB, which would operate according to content protection related con-

trol data transmitted along with regularly broadcast programmes. Digital broadcasting in Japan transmits encrypted content to achieve such enforcement, based on confidential data provided, including a decryption key. Such confidential information is provided in the form of an IC card (B-CAS card).

With regard to content protection and management, additional consideration should also be given to PDR that can record and reproduce digitally formatted programs without conversion (D-VHS, HDD, etc.). These recording and reproduction systems are designed on the premise of a high-speed digital interface (IEEE1394) connection, protecting digital content under a de facto standard (e.g. DTCP). For this reason, interfaces are also provided for transmitting content protection control data to recording devices and other systems over broadcast.

Regarding re-transmission to the Internet, a flag, or encryption mode, is prepared for a Content Availability Descriptor to enable receiver control.

The relationship between content protection and management requirements and a part of RMPI transmitted via broadcasting is described in the inserted *Table 1*. It prohibits a receiver from having the capability to send the designated contents, which either include a copy restriction by Digital Copy Control Descriptor's "digital recording control data" or has copy protection specified by the Content Availability Descriptor's encryption mode, to any output that could potentially allow the content to be re-transmitted over the Internet. Re-transmission to the Internet is prohibited in those cases where the encryption mode is "0" or copying is restricted by "digital recording control data.

Table 1: Copy control specification.

Contents protection requirements		Data transmitted via broadcast				Descriptor			output	
Digital Copy Control	Analog Copy Control	Digital Copy Control Descriptor operation			Content Availability Descriptor operation	Digital Copy Control		Content Availability Descriptor	Analog video	Digital audio
		copy_ control_ type	digital_ recording_ control data	APS_ control _data	encryption_mode	copy_ control_ type	digital_r ecording _control _data	Encryption_mo de		
Copy-freely	Copy-freely	01	00	00	0	01	00	1	CGMS-A: 00 Macrovision: off*	SCMS: Copy-freely
Copy-freely					1					
Copy-never	Copy-never. It can be copied only for conventional analog input recording, since Macrovision is not attached.		11	00	1			0	CGMS-A: 00 Macrovision: off*	SCMS: Copy-freely
	Copy-never.			Non-00	1					
Copy-one-generation	Copy-one-generation. It can be copied only for conventional analog input recording, since Macrovision is not attached.		10	00	1		10	Don't care	CGMS-A: 10 Macrovision: off*	SCMS: Copy-one-generation.
	Becomes Copy-never after one copy.			Non- 00	1		11	Don't care	CGMS-A: 11 Macrovision: APS	SCMS: Copy-never.

Bottom line

Digital broadcasting receivers will be distributed with a key for broadcast viewing, on the condition that they operate according to the signals transmitted via the broadcast. Thus Japanese digital broadcasting is scrambled but free to air. This situation differs from the US and the EU as it is accomplished by CAS technique. CAS is mandated for ARIB (STD-B25) standard receivers. Scrambling contents does not necessarily require mandating a broadcast flag like in the US because the contents are protected by CAS.

Sources

- Asia-Pacific Broadcasting Union (ABU) : http://www.abu.org.my/public/index.cfm
- Association of Radio Industries and Businesses standards: http://www.arib.or.jp/english/index.html; Relevant standards and guidelines developed are:

- ARIB STD-B10 Service Information For Digital Broadcasting System
- ARIB STD-B21 Receiver For Digital Broadcasting (Desirable Specifications)
- ARIB STD-B25 Conditional Access System Specifications for Digital Broadcasting
- ARIB TR-B14 Operational Guidelines for Digital Terrestrial Television Broadcasting
- ARIB TR-B15 Operational Guidelines For Digital Satellite Broadcasting

► BS Conditional Access Systems Co., Ltd.: http://www.b-cas.co.jp

► The Association for Promotion of Digital Broadcasting: http://d-pa.org

► The Association for Promotion of Satellite Broadcasting: http://www.bpa.or.jp

About the author: Kiyohiko Ishikawa received the Ph. D. degree in engineering from Nagoya University, Aichi, Japan in 2004. He joined Japan Broadcasting Corporation (NHK), Tokyo, Japan, in 1990, where he is now with the Science and Technical Research Laboratories. Since 1992, he has been engaged in research on magnetic recording head and media and signal processing for high-density magnetic recording systems and on broad-band and high-speed optical disk recording. He currently researches security system for digital broadcast based on home servers.

Status: first posted 25/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=166

The Sony BMG rootkit scandal
Consumers in the US finally wake up. And march to courts…

By: Natali Helberger, IvIR, Amsterdam, The Netherlands

Abstract: The article will have a closer look at the charges of the EFF and a Californian lawyer against Sony BMG's latest DRM strategy. The Sony BMG case adds a number of new dimensions to the DRM and Consumer debate. The article will highlight some aspects, also against the background of similar recent case law in Europe.

Keywords: legal analysis - consumer protection, data protection, DRMS, music industry, users - US

Introduction

Dark clouds are gathering above the US headquarter of Sony BMG in New York. Complaints are showering down on the enterprise. Class actions zig-zag the once so blue sky of the world's second largest entertainment company. Sony BMG is in deep trouble, and the forecasts are on "storm".

All this because of a small piece of software, Sony BMG's newest Extended Copy Protection technology - XCP, developed by First4Internet (cf. also the INDICARE Monitor article on intrusive DRM by Bohn 2005). Apparently, Sony BMG could not resist the temptation to pack more functionality into its DRM than is really needed to protect contents against unauthorised copying. After all, who would care? Or, to speak in the words of Sony BMG's global digital business division president *Thomas Hesse*: "Most people, I think, don't even know what a rootkit is, so why should they care about it?" (cited in EFF 2005). For those, who still do not know what a rootkit is: a rootkit is a piece of software that cloaks processes, files and logs from a computer's operating system or from its anti-virus programs with the effect that the owner of the computer will not notice that certain routines are performed on his or her computer, or that the software disturbs the transmission of data from terminals, CD drives or keyboards. Sony BMG's XCP installs, unnoticed by the user, a piece of software that prevents consumers not only from copying the content of a CD more often than the allowed three times. XCP recognises and registers the CD that is played on a computer, identifies the IP number of the computer, is able to monitor and report user behaviour

back to the firm, manipulates parts of the computer memory, crashes applications or the entire Windows operating system, interferes with file copying software and other media players and, accidentally, offers shelter for viruses, worms and other nasty things. Attempts to remove the software can lead to system crashes, malfunctions, un-usability of the CD drive and other damage at consumer's computers (Russinovich 2005a).

Luckily, somebody knew what a rootkit is, and could recognise one when he saw one. *Mark Russinovich*, chief software architect at Winternals Software Inc, discovered to his dismay that the Sony BMG CD "Get Right with the Man" by the *Van Zant brothers* installed not only an "underhanded and sloppily written" (Russinovich 2005a, but see also Hamm 2005) piece of software, but also a potentially harmful one. Russinovich documented his discovery on his blog, and the story soon made its way into the media. Comment from Russinovich: "This is the case of the blogosphere having an impact, at least for the moment" (Russinovich 2005b). The impact will be not just for the moment.

Class actions against Sony BMG based on consumer law

The first class action against Sony BMG on behalf of Sony BMG CD buyers was brought by a Californian lawyer, *Alan Himmelfarb*. One of the many things that is special about this case, is that, at least to the knowledge of the author, this was one of the first occasions that in the US an action on the basis of consumer law was brought against DRM. Until now, in the US the DRM discussion was generally kept in the copyright domain (see e.g. Liu 2003, Cohen 2005). Himmelfarb accused Sony BMG of the violation of Sections 1770 (a) 5 and 9 of the Californian Civil Code (this title in the Californian Civil Code is also known as the Consumer Legal Remedies Act; cf. sources). Section 1770 (a) 5 and 9 ban representing that goods or services have characteristics which they do not have, comparable to the European provision on misleading practices. According to Himmelfarb, by concealing the existence of the rootkit program, and what it does once installed on a user's computer, Sony BMG has violated both sections of the Californian Civil Code and has committed unfair, deceptive and misleading business practices.

Not content with that, the Electronic Frontier Foundation (EFF) brought a second class action complaint against Sony BMG's XCP technology. The EFF charge also includes the MediaMax technology used by Sony BMG. The EFF found that the MediaMax DRM has characteristics very similar to those of XCP. Again, the EFF claim is based on the Consumer Legal Remedies Act.

Scrutiny of the Sony BMG's EULA

In addition to the charge about misleading practices, the EEF complained about Sony BMG's provisions in the consumer contract, in form of Sony BMG's End User Licence Agreements ("EULA") for the XCP and MediaMax CDs. The EEF had a closer look at the EULAs and found, indeed, rather bizarre conditions:

- restrictions on the user's ability to use the digital content on the CD in the event that that consumer chose to leave the United States, *speak*: once you leave the country you are no longer allowed to listen to any of the CDs you purchased.
- restrictions on resale and transfer of the digital content on the CDs, *speak*: no way that you can get rid of your infected CD by selling it to your uncle or at the flee market.
- restrictions on the user's ability to use the digital content on the CDs at work, *speak*: you go to work, the music stays home;
- restrictions on the user's ability to use and retain lawfully made copies of the digital content on the CDs in the event that the original CD is stolen or lost, *speak*: should anybody nick your CDs, you are obliged to also delete all remaining copies that you might have made, as if you didn't have enough trouble already;
- restrictions on the user's ability to use the digital content on the CDs following a bankruptcy, *speak*: if you've lost your

money you're are not worthy to listen to Sony BMG music;

- conditioning the user's continued use of the digital content on the CDs on acceptance of all Sony BMG software updates, *speak*: you have to accept all updates that Sony BMG wants to smuggle onto your computer, or: forget about listening to your CD;
- restrictions on the user's ability to examine and test his or her computer to understand and attempt to prevent the damage caused by the rootkit, *speak*: maybe you have a bad feeling with that CD, maybe you are a second Russinovich, still, Russinovitch-like self-help actions are not part of your contract, sorry;
- a reservation of rights by Sony BMG to use "technological 'self-help' measures" against the computers of users who desire to make use of the digital content on the CDs "at any time, without notice to [the user]"; *speak*: Sony BMG reserves the right to happily install more anti-copying protection ever after, and you are not even entitled to know about it;
- and… and… and. (EFF 2005).

Without accepting the EULAs, consumers will have no access to the CD. This is hard, considering that they have already purchased the CD. It remains to be seen how the judge will decide. In the US, contractual freedom is a highstanding value, which makes it at least doubtful if the judge will find these restrictions unconscionable.

The two cases (and more are on the way; e.g. the Attorney General of Texas brings a suit against Sony BMG in Texas; cf. The State of Texas 2005) confirm once more that DRM is not only a matter of copyright law, but that it touches, much more broadly, on valid interests of consumers, those who purchase digital content for own, private use. EEF's allegations concerning MediaMax, moreover, show that the rootkit scandal was not simply an accident, but part of an established business strategy of one of the largest music publishers in the world. The cases are in line with earlier cases in Europe where consumers claimed that the CDs they bought were defective products, due to the restrictions imposed by the DRM (Helberger 2004, 2005 a, b). The Sony BMG case, however, adds a number of new dimensions to the existing experiences with claims against DRM. This is why it is interesting to look at some details of the claim more closely.

Unfair competition law

Interestingly, Californian law knows another provision. In Division 8 of the Business and Professions Code (cf. sources), i.e. California's unfair competition law, which was also evoked by both, Himmelfarb and the EFF against Sony BMG, Section 22947 contains what is called the Consumer Protection Against Computer Spyware Act (cf. sources). Unfair competition law plays an important role in terms of consumer protection in California, as it includes a number of consumer friendly provisions. The Consumer Protection Against Computer Spyware Act prohibits a person or entity other than the owner of a computer to insert without authorisation spyware on that person's computer, that is software that:

- takes control of the computer;
- modifies internet settings;
- collects personal information;
- prevents efforts to block the installation of that software;
- pretends that the consumer can de-install the software, if in reality she cannot do so;
- removes, disables or renders inoperative security, anti-spyware or antivirus software installed on this computer.

In other words, the law, which passed Senate in August 2004, seems to have been written with an eerie foresight of the Sony BMG case. European consumer law does not know any comparable rules. The closest to this are probably national provisions on computer tampering in national penal codes.

It remains to be seen how the Superior Court of the State of California will decide – if it will decide at all. Presently, there are strong indications that Sony BMG will do its best to avoid a decision and settle the cases brought against it. EFF requests that Sony BMG will be obliged to:

- widely and detailed publicise the potential security and other risks for consumers associated with XCP and MediaMax technology;
- cooperate fully with manufacturers of anti-virus or similar security tools to facilitate the complete removal of XCP and MediaMax from infected computers (something which is, so far, not possible);
- refund the purchase price of the CDs containing MediaMax or XCP and
- to refrain from further abuses.

The last claim is interesting insofar as it is not restricted to appropriate labelling, as was claimed in the EU cases. Instead, the plaintiff demands that Sony BMG will avoid further abuses, making evident that Sony BMG's invasive technology should not be accepted under any terms, even if consumers receive a prior warning.

Another interesting characteristic of the US cases is their nature as class action – an accepted procedural instrument under US consumer protection law. EFF pointed out, very correctly, that it would be impracticable and prohibitively expensive if all members of the class sued individually. The damages suffered by each consumer were relatively small, too small to justify the high expenses for individual prosecution in a matter that is as complex as the present case. As a result, consumers would probably not sue on an individual basis. Moreover, as EFF also pointed out, a multitude of individual claims poses a serious strain on the functioning of the court system. These are problems that are equally critical in Europe and render the instrument of consumer protection law in DRM cases less effective; the situation in Europe is complicated by the fact that most European member states do not acknowledge the instrument of class action.

Finally, to mention a third interesting detail and difference to the European cases: neither Himmelfarb nor the EFF sought to use consumer protection law as a means to protest against the restriction of usage possibilities through DRM (e.g. private copying) or to make an argument in favour of fair use. In contrast, DRM and the private copying exception were at the heart of most of the existing claims in Europe. To the knowledge of the author, no (successful) attempts have been made in the US so far to use such a thing as warranties law as a means to enforce the private copying exception (as was done in Europe). The author was rather puzzled about this finding and tried, subsequently, to identify if this difference is the result of US consumer protection law and policy, or if it is by accident that yet no action in this respect has been taken in the US.

The answer must remain somewhat speculative. Partly, the reason might have to do with the structure of US copyright, notably the fair use defence. Unlike in Europe, in the US there is little discussion about if copyright law conveys a right to private copying. It is widely acknowledged that fair use is an affirmative defence, not a right. However, because the fair use principle is far broader than the European private copying exception, and because fair use cases are able to accommodate different interests beyond the making of private copies, the fair use doctrine invites far more readily attempts to adapt copyright law in a way to accommodate user interests (Cohen 2005, Liu 2003), without seeking recourse to consumer protection law. This may explain, why in the US, the DRM discussion has concentrated so far mostly on the copyright domain.

On the other hand, its vagueness and the lack of a clearly encircled (that is: worded) protection worthy consumer interest (e.g. private copying) in US copyright law may be a reason, why consumer protection law is of little use to enforce an existing standard in copyright law. Such a standard simply does not exist, at least not in form of clearly carved out copyright exceptions. This observation leads to the other part of a possible answer, why US consumer protection law was not used so far to enforce user interests in e.g. private copying. The respect for contractual freedom and the contractual autonomy of private parties is particularly strongly developed in the US. In general, the idea is that the state should refrain from interfering with the actions of private parties as much as possible. In contrast, in Europe the concept of the

positive protection duty of the state, i.e. the state's duty to actively create an environment that is favourable to consumers' interests, is far more commonly acknowledged. Finally, in both, the US and Europe, a general idea prevails that consumer protection law protects in the first place individual consumer interests, and is less suitable to protect public policy interests, such as broad availability of services, stimulating creativity and innovation, etc.

Bottom line

The cases brought by Himmelfarb and the EFF are in many respects a primer. They also introduce us to the US consumer protection law as a possible remedy against DRM misuse, next to copyright law. We can await with suspense the decision by the Superior Court of the State of California, and whether it will trigger a wider reaching discussion about consumer protection in the IP sector in the US. One can hope so, because US law knows a number of interesting tools to improve the legal standing of consumers, be it the institute of class action, be it special rules about spyware. One the other hand, chances are high that this case of consumers suing an undertaking because of unfair practices will be, as so many others before it, settled before the judge will have a chance to make a final statement. Even so – some hairy questions are on the table! And, hopefully, they cannot be removed from there by simply giving each affected consumer a new CD or a voucher for some free downloads. This is about more than just a new CD.

Sources

- 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=155
- Cohen, J. (2005): The place of the user in Copyright Law, 74 Fordham Law Review (forthcoming)
- Consumers Legal Remedies Act: http://www.harp.org/clra.htm
- Consumer Protection Against Computer Spyware Act: http://pub.bna.com/eclr/sb1436.htm
- Division 8 of the Business and Professions Code: http://caselaw.lp.findlaw.com/cacodes/bpc/17200-17210.html
- EFF (2005): Class Action Complaint before the Superior Court of the State of California, County Los Angeles, available at: http://www.oag.state.tx.us/newspubs/releases/2005/112105sony_pop.pdf
- Hamm, S. (2005): Sony BMG's costly silence, Business Week Online, November 29, 2005, available at: http://www.businessweek.com/print/technology/content/nov2005/tc20051129_938966.htm
- Helberger, N. (2004): It's not a right silly! The private copying exception in practice. INDICARE Monitor, Vol. 1, no. 5, October 2004; http://www.indicare.org/tiki-read_article.php?articleId=48
- Helberger, N. (2005a): Thou shalt not mislead thy customer! The pitfalls of labelling and transparency,. INDICARE Monitor, Vol. 1, no 9, February 2005, http://www.indicare.org/tiki-read_article.php?articleId=76
- Helberger, N. (2005b): Not so silly after all. New hope for the private copying exception, INDICARE Monitor, Vol. 2, no 6, August 2005; http://www.indicare.org/tiki-read_article.php?articleId=132
- Liu, J. (2003): Copyright Law's theory of the consumer. Boston College Law Review, Vol. 44, 2003
- Russinovich, M. (2005a): Sony, Rootkits and Digital Rights Management gone too far. Blog, available at http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html
- Russinovich, M. (2005b): More on Sony: Dangerous decloaking patch, EULAs and phoning home; Blog, available at http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html
- The State of Texas v. SONY BMG Music entertainment, LLC (2005); http://www.oag.state.tx.us/newspubs/releases/2005/122105sony_lawsuit.pdf

About the author: Dr. Natali Helberger is senior project researcher at the Institute for Information Law, University of Amsterdam, and managing legal partner in the INDICARE project. Dr. Helberger specialises in information law, technical control of information, the interface between law and technology, and between media, intellectual property and telecommunications law. Presently, she is staying as visiting scholar at the University of California, Berkeley. Contact: helberger@ivir.nl

Status: first posted 09/01/06; licensed under Creative Commons

URL: http://www.indicare.org/tiki-read_article.php?articleId=165

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