



— *Information*

— *Libraries*

— *Democracy*

Proceedings & Abstracts

24th BOBCATSSS Conference

Proceedings & Abstracts

January 27–29 2016

Lyon, France

www.bobcatsss2016.com

Edited by Fanny Blanchard, Valentin Famelard, Katarina Leyrer, Guilhem Martin Saint-Léon, Paulin Ribbe, and Laure Fabre.

Published by Enssib, Villeurbanne, France, 2016.



Table of contents

Introduction.....	3
Table of contents	5
Papers.....	9
Public libraries as tools for democracy	10
Towards Better Social Learning: Contributions from Sentiment Analysis	21
Citizen Scholarship using Web2.0: Tools in Library and Information Science Journals	28
Diversity of film collections in European public libraries.....	37
Security level of DRM technologies	50
Youth as Citizen?: Libraries and Youth Civic Engagement.....	58
Hacker culture, libraries and intellectual freedom: Analysis of hacker and hacktivist scene in Croatia and its collaboration with Croatian libraries	67
French Libraries Post-Charlie Hebdo: Between Freedom of Expression and the Neutrality of Cultural Institutions.....	78
E-book reading data protection in libraries.....	93
Modern Times, Modern Librarians: A Comparison of Historical and Modern Library Services of Hungary and the United States.....	103
User Experience in the Italian Academic Libraries context: may we start?.....	110
Mobile library service in Baranya County: How to provide library services to the people of a rural region in Hungary?.....	118
An Analysis of International Library Aid to Africa: Cultural, Economic, and Political Impacts.	127
French think tanks analysts and librarians: the cart of communication comes before the horse of knowledge.....	135
Target Groups and Activities: Six Swedish Public Libraries' use of Facebook.....	145
Film education and film preferences of the LIS students as important factors for the development of diverse film collections.....	153
Green Libraries – partners for realizing fully citizenship	164

Social media and privacy defense strategies.....	176
Do Erasmus students have the same rights using library resources studying abroad?	185
Student's information needs in democratic society and the role of public libraries	196
Redesigning the physical space for access and exchange of knowledge: Tracking the Traffic at the University of Oslo Library.....	205
Librarian as publisher	215
Librarian's Code of Ethics - Does It Help?.....	221
The library as a stronghold of privacy in the digital age : a three-tier framework.....	223
Analysis of cultural events in the library with the aim of promoting literature.....	233
A Comparative Analysis of the State of Intellectual Freedom in the United States and Israel as Judged Against IFLA's FAIFE Committee Standards	246
Democracy in the works council libraries. A case study: The Social Welfare Institutions for staff in the electrical and gas industries (CCAS - France).....	254
Legal deposit at the Sultanate of Oman: the Law of Press and Publications and its role in building Omani culture democracy.....	264
Libraries on the Semantic Web: Finding new professional ways and implement them to the benefits of citizens	277
Is the library a true reflection of information's democracy?.....	285
Social Networking: Information Sharing, Archiving and Privacy	294
Censorship in the School Library: four reasons to consider and some ideas to promote Intellectual Freedom.....	315
The Role of Social Factors in the Design of Information Systems and Services for Open Data...	322
Disseminating knowledge beyond scholarly journals: coverage of Library and Information Science literature in Wikipedia.....	332
How Can Public Libraries Support Active Citizenship and Regional Vitality? Case Study: Vallila Library, Helsinki City Library.....	342
Living libraries: a commitment to think and transform the city.....	349
Open Science as a Service: Status and future potential from a German non-university research institution perspective.....	356
Information values in conflict: How libraries navigate occasions of dissonance between freedom of information and the right to privacy.....	366
Enforcing and Reinforcing the Responsibility of Information Professionals to Defend Intellectual Freedom. The Role of Positive Reinforcement instead of Sanctions in promoting Intellectual Freedom.....	375

Student-teacher Facebook friendship and privacy awareness.....	383
Posters.....	395
How your library can help to set you free from mass-surveillance?.....	396
Living Library in Reader Development.....	398
Video Streaming in Academic Libraries: Enabling Participation in a Democratic Society.....	402
The Search That Dare Not Speak Its Name: LGBT Information and Catalog Records.....	407
Syrtis: New Perspectives for Semantic Web Adoption.....	412
Libraries, Pornography, and the Internet: An Evolving Conversation	417
Accessible safe Internet for children: project of Russian libraries	421
The Role of Public Libraries in Communities Impacted by Natural Disasters.....	423
BOISSY Archive: an innovative project which seeks to develop the reflection on text-markup standard to enhance research in French eighteenth century theater.....	429
Design thinking for libraries — Libdesign project.....	434
“I Go There If I feel Welcome”: Use of Czech Libraries by Immigrants.....	441
To offer ebooks in libraries: a way to break down physical barriers to knowledge and culture ...	445
Community Oriented Libraries and the Third-Space in African Libraries.....	451
The Panoptic Principle and Information Access in UK Public Libraries.....	458
Intellectual freedom and censorship in Norwegian public libraries.....	464
Public Libraries and E-Democracy	466
Workshops.....	473
The Declaration of Lyon an international tool for a local action?	474
The Cross-border Copyfight, A copyright workshop for library professionals.....	479
Libraries and refugees, Les bibliothèques et les réfugiés : reaffirmation of a social and political role.....	481
Facebook, WhatsApp, what else? Social media and search engines: Do we need alternative systems?	484
Be an Open Scientist	487

Government documentation and open government in the library: from transparency to empowerment.....	488
Afripédia: rebalancing access and visibility on Wikipedia.....	490
How tablets can help children with learning disabilities.....	492
Technical Challenges to Privacy: Practical Training for Librarians	494
Ethics for Information Professionals	496
Role playing in Libraries: promoting reading for children	499
Global Trends, Local Voices: Libraries responding to the IFLA Trend Report.....	501
Data curator: who is she/he?.....	504
Super-Open Librarians: become the new heroes of a free and open information strategy	507
Intellectual freedom versus internet providers.....	510
Get related 2.0.....	513
Thematical table of contents.....	516
Relive the symposium day by day!.....	523
THURSDAY 28 - ENSSIB	523
FRIDAY 29 - ENSSIB.....	528
Scientific committee.....	532
Organization Bobcatsss 2016.....	533
Sponsors	535
Index	537



Papers



Security level of DRM technologies

Zsuzsanna Arany, Andor Nagy

arany.zsuzsi19@gmail.com, donandor@gmail.com

University of Pécs - Faculty of Cultural Sciences, Education and Regional Development, Hungary - 7633 Pécs, Szántó Kovács János u. 1/b.

Keywords: *Ebook, DRM, Security, Vulnerability*

Abstract

One of the greatest challenges libraries are facing in the recent years is developing e-book related services. Given that these are present on the market in ever increasing numbers, the task to reconcile conflicts of interests that are hindering library service is growing more urgent by the minute. Most entities on the market regard the DRM (Digital Rights Management) technologies as the solution, though the publishers do not trust their efficiency. The goal of DRM is to stop illegal circulation of e-books bought or rented from a legal source.

Many of the largest corporations have developed their own DRM solutions, and as such, libraries and bookstores have the option to choose from many different solutions. However, owners of intellectual property, being afraid of online piracy, are still reluctant when it comes to spreading their works in electronic form (this is especially true related to borrowing from a library).

The aim of this research is to give an insight for those interested in the topic and stakeholders involved in publishing e-books into the operation of certain DRM technologies, an overview of the differences between them and an answer to the question of whether the fear of the publishers from pirated copies is valid. I will focus on the process of operation and possible security-related vulnerabilities of certain DRM solutions.

Furthermore, I will pose the question of whether it can be said in general of DRM solutions that they do not successfully obstruct piracy, or whether any exceptions exist. Having carefully examined the different DRM technologies I arrived to the conclusion that none of them can efficiently fulfill its mission, consequently owners of intellectual property have to find other means to protect their values against illegal distributors when designing library services.

In recent years, electronic texts have become more and more common. They have been around for some time, but as information technology is progressing, so are devices that can display electronic documents. This process enhances the demand for readers and electronic documents in general, which is of crucial importance for libraries and bookstores. Electronic documents present these institutions with an absolutely new challenge: although traditional, paper-based document services are well established by now, dealing with electronic documents raises several questions. They are primarily related to copyright issues, since one of the attributes of electronic documents is that they can be copied very easily. This is an appealing feature for readers, but the owners of copyright-protected documents are worried to publish their work electronically. Some authors, like Stephen King, do not publish some of their writings or they make them electronically available with a delay. Others do not want to be left out of e-book publishing, so they make their work electronically accessible and trust the technologies designed to prevent illegal sharing. My research focuses on the effectiveness of DRM technologies.

The question of whether it is worth using DRM technologies and which method is the most secure has been around for a while. Some believe DRM technologies are secure and are willing to spend hundreds of thousands of Euros on them, while there are also skeptics who avoid electronic publishing altogether. DRM technologies have been designed to protect intellectual property. They are not very new - even magnetic tape mediums were equipped with protection mechanisms. DRM technologies are, of course, more complex. Apart from protecting copyrighted content from copying, they can also be used to limit renting time - when the time expires, the document can be made unreadable.

My research focuses on the examination of the operation and vulnerability of DRM technologies from the point of view of informatics, rather than giving a general review. My hope with this study was to find an answer to the question if DRM technologies are worth relying on in the future when selling and lending electronic books. Also, if they prove to be reliable, which method is the most secure? Altogether, I have examined eight techniques which are being regularly developed.

Due to the specific nature of my research, I had very little literature available, so I had to search for other ways to study the operation and discover the flaws in DRM solutions. I have been able to find documentation for some DRMs, though. This documentation is intended for the clients' IT specialists, and they contain detailed instructions on how to integrate the technology into their current systems. I have had some extremely positive experience with BooXstream DRM after contacting the developer - he readily answered a few technical questions and sent me the documentation as well. Studying it proved to be very helpful for finding out more about the operation of DRMs, but they were not available for all the technologies, and the one I received was insufficient for a comprehensive study.

I used three methods: studying the documentation, analyzing various DRM protection softwares, and, in some cases, finding out about the operation of software designed to remove DRM protection. The basis of my research was the examination of DRM protection software and the analysis of program codes designed to by-pass it. Since, in most cases, DRM is not freely accessible, open source software, I had to find indirect ways to understand their operation and reveal their weaknesses. For example, when we open a program, a large number of system files are created on the hard drive and the memory. Despite these files being temporary (i.e. they are only needed for the current running of the program), they can be tracked down and provide insight into file functions carried out by the program. Valuable information can also be gathered by observing the network cards data-traffic while the DRM software communicates with the authentication server.

Another great help was the examination of software made to remove DRM protection. Most such software is open-source, the program codes were freely accessible, and by studying in detail the circumstances of executing these codes provided me with invaluable information.

Due to time constraints, I am going to report only my findings about the most widely used software Adobe ADEPT, and then summarize the rest of my research. I have chosen to focus on Adobe ADEPT because it is the most common DRM software and it is thought to be the most reliable by many. The full report of my study can be read in the latest issue of “Könyvtári Figyelő”.

The Adobe DRM solution has **3 key participants**: The **reader**, whose reading device runs Adobe Digital Editions, which can open the purchased or rented e-book. This software is in touch with the **Adobe Content Server** run on the server of the library, as well as with the **Adobe Authentication Server**. These three participants communicate several times during the authentication process.

For example, when an e-book arrives at a library and is added to the holdings, the **Adobe Content Server** encrypts it with a particular document key and from then on each time someone rents the e-book, it is encrypted with the same key.

Although the reader receives this key with the e-book, it comes in a format that only the Adobe software can interpret. This is achieved by each registered reader having their own user key, based on which an algorithm creates a new key, which encrypts the document key received. Thus, by the time the reader gets the key, it has been encrypted several times.

The entire process takes place like this:

When the reader buys or rents an e-book, they do not receive the document itself but a tiny file with ACSM extension, which is an XML type document. It contains the basic data of the e-book, including the URL which the readable e-book will be downloaded from after the authentication process is completed.

When the reader opens the ACSM file on their own reading device, Adobe Digital Editions sends 4 things to Adobe:

- the reader's personal identity code;
- the identity code of the reading device (for example the hard drive serial number, the identity code of the processor, or the so called MAC address of the network card);
- the reader's unique personal key;
- and the identity code of the requested e-book.

The identity code of the e-book is not only sent to the Adobe server, but also to the library. In response, the library requests the e-book key from Adobe, as it is only to be found on the Adobe server.

As the last step, Adobe Digital Editions running on the reader's reading device creates the key that Adobe has encrypted the document key with; basically, we can say, it copies the key needed to decrypt the document key. Once the process is complete and the document key is available, the e-book itself becomes readable. The essence of this process is that the reader cannot access the unencrypted e-book since the entire authentication process is carried out by Adobe's own servers, without letting the reader know what processes are taking place in the background.

The flaw in the process:

Although Adobe has created an extremely complex DRM process, it contains a flaw: despite the strict rules and the complicated authentication process, the e-book and its document key do get onto the reader's device. This would not be a problem in itself, since both the e-book and the document key are encrypted and unusable on their own. However, it is not impossible to unlock the document key encryption - several programs have been designed to do that. In order to unlock the encryption, we need to examine how the key was encrypted. This can be done with the so called reverse engineering method, which means the decryption process carried out by the reading software is analyzed step by step. With the obtained data we can model the process, so, besides the Adobe software, software designed to decrypt will also be able to unlock the encryption and we will have a DRM-free document as a result.

Let us take a closer look at the reverse engineering method in order to see what it can reveal about the process:

As the first step, the encrypting software gets the reader's unique personal key. Then it removes part out of it to make it harder to identify, which is a way of distraction.

This truncated key is encrypted in two layers, applying the base64 process first and then the 128-bite *Advanced Encryption Standard* coding. The flaw of this two-layer encryption method is that base64 is a reversible code form and is easy to do; the *Advanced Encryption Standard would be safe enough in itself, however, the decryption key is stored on the reader's computer by the Adobe software.*

So if we do this process backwards, that is we decrypt the Advanced Encryption Standard and then the base64 code, we can access the document key.

I have shown the flaws in only one method, but in my full paper I present in detail the security flaws in Apple FairPlay, Barnes and Noble, Marlin, BooXstream, SiDiM and Amazon mobi, and DRM solutions used with topaz format e-books. The flaws in FairPlay result primarily from the simplicity of the encryption algorithm and in the fact that the reader's device communicates with Apple's central server through an insecure channel. Barnes and Noble create the key in an even simpler way, in two steps. Marlin DRM operates very similarly and also stores the elements of the key in a SQLite database on the reader's device. BooXstream uses a completely different method - various watermarks - but does not come up with any revolutionary solution, so detecting the watermarks is not impossible either. However, SiDiM places watermarks differently: for example, by slightly modifying the phrasing and by changing word order in sentences so that the sentences still remain meaningful. The flaw in this method results from the fact that the modifications are done differently for each reader, so if two copies of the same e-book are compared, most changes can be detected – this way it is difficult to identify a reader securely. In addition, after its unfavorable reception, it seems that SiDiM will not be further developed. Finally, Amazon uses DRM for two file formats, mobi and topaz. In both cases, the algorithm used to create the key is so simple that the key can often be unlocked by simple trials (brute force method).

My study has shown that all the 8 DRM technologies I have examined, including Adobe ADEPT, can be bypassed. In most cases a security breach does not only exist in theory, but there is publicly available software capable of removing the DRM in question. There are some protection methods with no public solutions for bypassing them, but even these have flaws, and if they become more widespread, it is most probable that someone will share software to remove the protection.

Based on this information I think the use of DRM is not a real solution to prevent the promotion of pirate copies, as soon as only one person removes the protection from a document and then publishes the e-book on a file sharing site, the money spent on DRM technology has been wasted. Furthermore, the use of DRM technology has a downside, too. If a person buys or rents a protected document, there are several restrictions on its use, for example, the document cannot be copied freely, it can only be read on certain devices or it

cannot be printed. As opposed to this, an illegal copy can be used freely, which makes it more attractive for readers in at least two ways: it is free, and its use is unrestricted.

The conclusion of my study is that currently there is no DRM technology that can effectively protect documents from pirate copying and sharing, therefore I think its use has no real advantages. Moreover, due to the lack of restrictions, pirate copies are more appealing, which also makes the use of DRM ineffective. In my view, a new method should be developed to promote legal e-book consumption.

References

- Abie, Habtamu (2007). Frontiers of DRM Knowledge and Technology. *International Journal of Computer Science and Network Security*, 7 (1), 216-231.
- Adobe Inc. (2009). Adobe and Barnes & Noble Join Forces to Standardize eBook Technology. Retrieved: August 30, 2014. https://www.adobe.com/aboutadobe/pressroom/pressreleases/pdfs/200910/102009AdobeBarnesNoblebooks_000.pdf
- Adobe Systems Incorporated (2009). Adobe Content Server 4 User Manual. [not public document for customers]
- Ausderau, Patrick (2014). *Protection mechanisms for electronic books*. Helsinki: Helsinki Metropolia University of Applied Sciences. Retrieved: July 21, 2014. [doctoral thesis] https://www.theseus.fi/xmlui/bitstream/handle/10024/74667/Ausderau_Patrick.pdf
- Bailey, Jonathan (June 18, 2013). Changing Words and Changing Direction on eBook DRM. *PlagiarismToday.com*. Retrieved: August 15, 2014. <https://www.plagiarismtoday.com/2013/06/18/changing-words-and-changing-direction-on-ebook-drm>
- Bangor University's Languages Technologies Unit (2012). E-publishing: Technical guidelines for Publishers in Wales. Retrieved: August 15, 2014. http://techiaith.bangor.ac.uk/e-gyhoeddwr/wp-content/docs/E-publishing-Technical_Guidelines.pdf
- Biryukov, Alex - Leurent, Gaëtan - Roy, Arnab (2012). Cryptanalysis of the "Kindle" Cipher. Luxembourg. Retrieved: July 25, 2014. http://www.di.ens.fr/~leurent/files/Kindle_SAC12_slides.pdf
- Bodó Balázs (2010). A DRM-mítosz - mire jó és mire nem a másolásvédelem. *Könyvmarketing konferencia*, Budapest. Retrieved: December 7, 2014. <https://prezi.com/ecqe-mxidnuz/konyvmarketing-2010>
- DeMarco, Amanda (2012). BooXtream on "Social DRM" as a Better Option for E-books. Retrieved: October 25, 2014. <http://publishingperspectives.com/2012/09/booxstream-on-social-drm-as-a-better-option-for-e-books/>

- De-Mulder, Yoni (2014). White-Box Cryptography. Belgium. Retrieved: July 25.
2014.<https://www.cosic.esat.kuleuven.be/publications/thesis-235.pdf>
- Digital Watermarking Alliance (2007) Digital Watermarking as a Proposed Solution to Orphan Works. Retrieved: September 5,
2014.http://www.digitalwatermarkingalliance.org/docs/papers/dwa_whitepaper_OrphanWorks.pdf
- ECDLweb (2010). A számítógép működési elve. *ECDLweb*. Retrieved: March 10,
2015.http://ecdweb.hu/A_sz%C3%A1m%C3%ADt%C3%B3g%C3%A9p_m%C5%B1k%C3%B6d%C3%A9si_elve
- Iannella, Renato (2001). Digital Rights Management (DRM) Architectures. *D-Lib Magazine*, 7 (6). Retrieved: August 30, 2014. <http://www.dlib.org/dlib/june01/iannella/06iannella.html>
- Intertrust (2011). Marlin Broadband Architecture Overview. Sunnyvale. Retrieved: August 10,
2014.<http://www.marlin-community.com/public/MarlinBroadbandArchitectureOverview.pdf>
- Intertrust (2012). Marlin Tutorial. Sunnyvale. Retrieved: August 14, 2014. <http://www.marlin-community.com/files/MarlinTutorial2012.pdf>
- Kantarciogluu, Murat (2008). Advanced Encryption Standard. The University of Texas at Dallas: Richardson. Retrieved: October 22,
2014.http://www.utdallas.edu/~muratk/courses/crypto09s_files/aes.pdf
- Kar, Saroj (August 19, 2013). A Look At SiDiM: A Thought for E-book DRM to Stop Piracy. SiliconANGLE.com. Retrieved: August 15, 2014. <http://siliconangle.com/blog/2013/08/19/a-look-at-sidim-a-thought-for-e-book-drm-to-stop-piracy>
- Mahmoud-Aref-Abadi, Imad (2008). Digital Rights Management for Personal Networks. London: University of London. Retrieved: July 26, 2014. [doctoral thesis]<http://digirep.rhul.ac.uk/items/231c27e9-a35c-9f96-36fd-25e4a2b9315b/1/RHUL-MA-2008-17.pdf>
- Moldován István (2014). E-könyvek, e-szövegek, könyvtárak. *Könyv és Nevelés*. 16 (3). Retrieved: March 5.
2015.http://olvasas.opkm.hu/portal/felso_menusor/konyv_es_neveles/ekonyvek_eszovegek_konyvtarak
- Ott, Matthias-Christian (2010). Digital Rights Management. Leipzig: Universität Leipzig. Retrieved: July 25, 2014. <http://www.informatik.uni-leipzig.de/~graebe/Texte/Ott-10.pdf>
- Perrin, Chad (April 17, 2009). Hacker vs. cracker. TechRepublic. Retrieved: March 5.
2015.<http://www.techrepublic.com/blog/it-security/hacker-vs-cracker>
- Qiang, Hao (2003). E-book Security: An Analysis of Current Protection Systems. Linköping: Linköping University. Retrieved: July 26, 2014. [doctoral thesis]. <http://liu.diva-portal.org/smash/get/diva2:19203/FULLTEXT01.pdf>

- Reuters (August 29, 2011). Marlin Community Announces Availability of eBook DRM Specification. Reuters Online. Retrieved: August 30, 2014.<http://www.reuters.com/article/2011/08/29/idUS142116+29-Aug-2011+BW20110829>
- Rothman, David (September 20, 2009). Barnes & Noble adopts open EPUB eBook Format, PDF and Adobe Content Server. TeleRead.com. Retrieved: August 30, 2014.<http://www.teleread.com/ebooks/barnes-noble-adopts-open-epub-ebook-format-pdf-and-adobe-content-server>
- Schultz, Rod (2012). The Many Facades of DRM. Retrieved: July 26, 2014.http://www.whiteboxcrypto.com/files/2012_MISC_DRM.pdf
- SiDiM (2011). SiDiM: Sichere Dokumente durch individuelle Markierung. Retrieved: July 26, 2014.https://www.sit.fraunhofer.de/fileadmin/dokumente/Projektblaetter/SiDiM_de.pdf
- Stallman, Richard (2003). Some Confusing or Loaded Words and Phrases that are Worth Avoiding. Retrieved: July 25, 2014. <http://www.gnu.org/philosophy/words-to-avoid.html>
- Torres-Padrosa, Víctor (2008). Contribution to an Architecture for Multimedia Information Management and Protection Based on Open Standards. Barcelona: Universitat Pompeu Fabra. Retrieved: July 26, 2014. [doctoral thesis].<http://www.tdx.cat/bitstream/handle/10803/7547/tvtp.pdf;jsessionid=FEA5C976E256FB63618D184678B73CAD.tdx2?sequence=1>
- Tószegi Zsuzsanna (2006). A szerzői jogok védelmét szolgáló digitális technológia. Tudományos és Műszaki Tájékoztatás, 53 (10), 447-456. Retrieved: September 27, 2014.http://tmt.omikk.bme.hu/show_news.html?id=4533&issue_id=476
- Van de Pol, Huub (2014). BooXtream Usage Scenarios. [not public document for customers]
- Van de Pol, Huub (2014). eBook Watermarking and Personalisation Distribution Platform. [not public document for customers]
- Van de Pol, Huub (2014). Pricing BooXtream™ Web Service. [not public document for customers]

