Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Digital Rights Management Overview

Digital rights management (DRM) refers to protecting ownership/copyright of electronic content by restricting what actions an authorized recipient may take in regard to that content. DRM gives digital-content publishers the ability to securely distribute high-value content such as periodicals, books, photographs, educational material, video, and research and to control the use of that content, preventing unauthorized distribution. [Noakes-Fry, Oct 2000] This paper presents an overview of DRM issues addressed, standards...

Copyright SANS Institute
Author Retains Full Rights

AD

DIGITAL RIGHTS MANAGEMENT OVERVIEW

Austin Russ

Security Essentials v1.2e

July, 2001

Introduction

Digital rights management (DRM) refers to protecting ownership/copyright of electronic content by restricting what actions an authorized recipient may take in regard to that content. DRM gives digital-content publishers the ability to securely distribute high-value content such as periodicals, books, photographs, educational material, video, and research and to control the use of that content, preventing unauthorized distribution. [Noakes-Fry, Oct 2000]

This paper presents an overview of DRM issues addressed, standards, technology and service providers, challenges, and guidance for determining if DRM may be applicable to your organization.

Background

While the phrase Digital Rights Management (DRM) is fairly new, the business challenges it targets are not. The economics of putting content online without a guaranteed return is moving content providers to re-examine their business models. Online advertising has not generated the anticipated revenues. As a contingency, online news and commentary sites are evaluating scaling back their operations or are considering charging for their content. DRM technologies allowing control over content use may be an attractive option for those considering making their sites pay-to-view. [Amis, 2001]

Roughly 70 years ago recording studios filed lawsuits to stop radio stations from illegally broadcasting their content—recorded music—for free. Twenty years ago, Hollywood claimed that inexpensive consumer VCRs would undermine its core business of making movies. In hindsight, these market disruptions signaled new market opportunities. Hollywood today reaps more revenues from video sales than from first-run movies. Radio proved to be the perfect marketing vehicle for promoting new music recordings and artists. [Intertrust]

In July, 2001, Metallica and rap artist Dr. Dre settled their copyright suits against Napster. As part of the agreement, Metallica will allow some of the band's songs to be traded on Napster's song-swap system once a legal business model has been launched. Napster's service has been off-line since July 2 as the company tries to retool its software technology to comply with the court order. [DailyNews, 2001]

Industry Perspectives

Napster's legal battles and the proliferation of "free" content on the Internet highlight two views on intellectual property protection in the Internet era. These views are expressed in Robert McGarvey's article for MIT Technology Review.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> *"I'm not convinced content can be protected in the Internet era," says Eric Scheirer, who tracks DRM issues for Forrester Research. "People want flexible access to content." Proof is Napster, of course, which represents a phenomenon Scheirer calls "unstoppable." Even if Napster is put out of business by the courts, he predicts that the frictionless distribution of digital content among the millions of Internet users will live on.* [McGarvey, 2001]

Internet Freedom http://www.netfreedom.org/default.asp is opposed to all forms of censorship and content regulation on the Internet.

> *DRM technologies may seem to be good news for content owners, be they record companies, movie studios, news organizations or online publications. However, the inevitable consequence of the implementation of DRM technologies is inconvenience and needless restrictions for users of digital media and the Net.* [Amis, 2001]

Conversely, Ranjit Singh, President of ContentGuard (a provider of DRM technologies) presents a case for the success of intellectual property protection.

> *Singh is betting heavily that DRM will prevail and, ironically, he thanks Napster. "Napster turned this whole issue into a CEO-level question. The very highest corporate officers now are looking into content management issues, and they want to protect their property."* [McGarvey, 2001]

Which view will materialize? Gartner Group envisions a six-year time horizon for DRM evolution and anticipates critical acceptance to be determined by 2003. The table below is adapted from their market assessment. [Weintraub, 2001]

Gartner Group's Timetable for DRM [adapted from: Weintraub, 2001]	
Year: Stage of DRM Evolution	**Characteristics of Stage**
2000: Education	• DRM vendors earn little or no revenue, most survive on their venture capital • Most vendor time and money spent on educating potential customers on the merits of DRM • Music industry evaluates DRM technology but questions remain about consumer acceptance
2001 - 2002: Early Adoption	• Experimentation, pilot projects • Cost models and issues need to be explored and stabilized • Business-to-business (B2B) and business-to-

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

	consumer (B2C) applications are piloted • User perceptions of ease of use must be addressed
2003: Production Launches	• Critical year for DRM adoption • Success of early implementations should indicate the strength of DRM demand and point to leading vendors • DRM vendors will partner with document management vendors to manage and control content across its life cycle
2004 - 2005: Growth and Maturity	• DRM vendor revenue models will stabilize • Core functionality will stabilize and additional enhancements will differentiate solutions
2006: Market Consolidation	• Standardization of rights language commoditizes DRM, weak vendors are acquired or disappear • Vendors seek differentiation through partnerships and/or vertical applications

Markets Targeted

Any business that needs to control access to and use of its intellectual property is a potential user of DRM. Gartner Group identifies six basic markets for DRM solutions [Noakes-Fry, October 2000]. These are listed in the table below.

Gartner Group's Markets for DRM [adapted from: Noakes-Fry, October 2000]	
Potential Markets	**Primary Business Risk Addressed**
1) Textbook Publishers and University Bookstores	Combat piracy
2) Providers of music, games, and other electronic entertainment	
3) Law Firms	Control access to information and ensure that the secure content reaches those parties who are accountable for its application or implementation.
4) Health Providers	
5) Financial Organizations	
6) Corporate Operations Departments	

Of these, Music and Publishing are positioned to lead DRM evaluation and adoption. The music industry is driven by recent legal actions to preserve their copyrights and control e-music. Publishing is seeking applications that allow extension of their traditional print distribution to e-content. [Weintraub, 2001]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

How DRM Solutions Work

While specific technologies and standards continue to evolve, Adobe provides a general description of how DRM works:

> *Effective DRM technologies work by allowing distributors of electronic content to control viewing access to the content - whether printed matter, music, or images - with some form of customized encryption. Individual "keys" for viewing or listening to the content are provided to an end user who has purchased rights, which generally include limitations on copying, printing, and redistribution.*
>
> *When a prospective owner of digital rights downloads a content file, DRM software checks the user's identity, contacts a financial clearinghouse to arrange payment, decrypts the file, and assigns a key - such as a password - for future access. The publisher of the content can configure access in numerous ways. For example, a document might be viewable but not printable, or may only be used for a limited time. (Peruse the "Digital Content for eCommerce" white paper for a discussion of various distribution scenarios and their business implications.)*
>
> *On the back end, things get even more complex. Once access rights and mechanisms have been assigned to a user, distributors must ensure that everyone in the creation, production, and distribution process gets paid fairly for use of the content. End-to-end software solutions, such as the MetaTrust Utility from InterTrust, track payments all the way from the online credit-card transaction to the royalty checks being deposited in the author or artist's account*
>
> *Most DRM experts agree that the best rights systems combine software and hardware access mechanisms. By tying access rights directly to computer CPUs, hard drives, or other storage media, publishers can control not only who is reading the information but also on what device. This level of protection is important for highly sensitive documents such as legal documents or proprietary market research, where illegal copying and sharing could result in substantial damages.*
>
> *Source: [Adobe, DRM]*

Emerging Standards

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Most emerging DRM standards focus on using Extensible Markup Language (XML) to describe the rules for controlling access to content. XML is a "metalanguage" that defines document structures and elements based on tagging information to be used for specific applications. XML is expected to take the lead over Hypertext Markup Language (HTML) for publishing applications. [Noakes-Fry, October 2000]

The XML Cover Pages http://xml.coverpages.org/sgml-xml.html is an online reference work for the Extensible Markup Language (XML). Searching the site for the phrase "digital rights management" identified a number of emerging standards listed in the table below.

Emerging Standard	Notes
Digital Property Rights Language (DPRL) Link: http://xml.coverpages.org/dprl.html	DPRL represents early Xerox research that evolved into XrML. See ContentGuard's homepage http://www.contentguard.com/for additional information on XrML.
Electronic Book Exchange (EBX) Working Group Home: http://www.ebxwg.org/	A standard for protecting copyright in electronic books and for distributing electronic books
Extensible Access Control Markup Language (XACML) Home: http://www.oasis-open.org/committees/xacml/	OASIS, the XML interoperability consortium announced in April 2001, *"XACML will define the representation for rules that specify the who, what, when and how of information access," explained Simon Y. Blackwell of Psoom, chair of the OASIS XACML Technical Committee. "Access control, which is often called 'rights management' or 'entitlement management,' determines who can look at something, what they can do with it, the type of device they can look at it on, etc."* http://www.oasis-open.org/news/oasis_news_04_24_01.shtml
Extensible Rights Markup Language (XrML) Home: http://www.xrml.org/	The xrml.org home page indicates, *"ContentGuard™ has developed and contributed XrML as an open specification licensed on a royalty-free basis to unify the Digital Rights Management industry and encourage inter-operability at an early stage."*
MPEG Rights Expression Language Home: http://www.cselt.it/mpeg/	Requirements, published in June 2001, are available at http://xml.coverpages.org/Reuters-mpeg-response-v10-public.pdf

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Open Digital Rights Language (ODRL) Home: http://odrl.net/	The latest version (0.9) was published in June 2001 and supersedes the previous draft of November 2000
Open eBook Forum (OeBF) Home: http://www.openebook.org/	Representatives of the Open eBook Forum and the Electronic Book Exchange (EBX) Working Group met during the week of December 4, 2000, and developed a plan to combine their efforts.
Secure Digital Music Initiative (SDMI) Home: http://www.sdmi.org/	This initiative has lost much interest. For details refer to "Why Secure Digital Music Initiative is Falling Apart" http://www.idg.net/spc_411846_6274_1-3861.html

Technology and Service Providers

A representative list of providers delivering DRM technologies and solutions to market appears in the table below.

Technology/Solution Provider and URL	Summary of Offerings (adapted from vendor web sites cited)
Technology Providers	
Adobe http://www.adobe.com/	• Adobe Content Server supports both PDF Merchant and EBX digital rights management schemes
InterTrust Rights|System http://www.intertrust.com/	• Rights|Packagers – content packaging for multiple media types and formats • Rights|Servers – authorization generator, content rights server, membership rights server, system operations server • Rights|Clients – trusted environments for governing content usage on clients, e.g., desktop, TV, phone, portable devices, PDF plug-in • Rights|Toolkits – tools for development and integration of DRM products • Hardware technologies include Rights|Chip and TrustChip
Solution Providers	
ContentGuard (a Xerox, Microsoft joint venture) http://www.contentguard.com/	• RightsEdge Platform - ContentGuard DRM technology consists of a RightsEdge Software Development Toolkit (SDK), applications and a back-office server to manage the life cycle.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

	• RightsEdge Services – ContentGuard offers consulting, training, outsourcing, support center services, and clearinghouse support. • RightsEdge Solutions - ContentGuard tailors solutions for customers • ContentGuard eContentPackager – a Web interface enabling content owners and retailers to protect eContent, establish pricing models and specify metadata. Examples of rights include time expiration and limitation of printable copies. • ContentGuard eContentSeller - A Web storefront that serves as the foundation for 24-hour distribution networks for eContent (currently supporting PDF and LIT eBook formats). It interfaces with companies like CyberCash for financial clearing.
IBM	• Content Manager http://www-4.ibm.com/software/data/cm/index.html • Electronic Media Management System (EMMS) http://www-4.ibm.com/software/is/emms/library.html
Reciprocal Inc. http://www.reciprocal.com/	• "*We build on the core technologies of today's leading providers, including Adobe® Systems, IBM®, InterTrust® Technologies Corporation, Microsoft®, and Preview Systems™. So you choose the best platform for your business--from the best platforms in the business.* "
Outsourcers	
Authentica http://www.authentica.com/	• Authentica focuses on B2B control over the use and distribution of three forms of digital content: e-mail, documents and web pages.
TrustData Solutions (formerly ASPSecure) http://www.aspsecure.com/	• Trusted Messaging Suite • Software Distribution Manager • Healthcare Info Manager • TrustData Services

With Microsoft backing, ContentGuard software will be included in Windows Media Player and in the Microsoft Reader for electronic books. (However, at this time, ContentGuard only applies to eBooks.)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

For broader solutions, Gartner Group reports, Reciprocal has no competitor that currently offers the same flexibility of services across multiple industries and multiple DRM platforms. [Noakes-Fry, January 2001]

Managing Expectations

Buzz-value aside, DRM products are not a "quick fix." Technology tools do not take the place of clearly expressed policy, which is then enforced by security hardware and software. Gartner Group estimates, implementing and integrating a DRM solution can take from three to 12 months and may require the outside expertise of a consultant.

Once implemented, there's no guarantee these protections won't be hacked. In "Secrets & Lies", Bruce Schneier writes:

> *The success of software pirates doesn't stop companies from trying to copy-protect their programs. The 1996 Quake release came on an encrypted CD-ROM: You could try it for free, but had to call the company and buy the password to unlock the entire game. It was eventually cracked, along with every other popular copy-protected program ever released.* [Schneier]

And, DRM may not always be the right solution for the problem.

> *What's really interesting about the problem of copy protection and software piracy is that the solution is to pretend that there's not a problem. There is little to no copy protection in business software. In the competitive software application industry, market share and product loyalty – no matter how they are achieved – are crucial. Many companies reason as follows: People who pirate my software cost my company next to nothing, since my marginal cost of goods is zero. It's not like they are stealing televisions off my assembly line. Almost all people who pirate my software can't afford to pay for it, so I'm not losing many sales. And, when these pirates eventually get into a situation where they need to buy the software legitimately, they will already be hooked on my software, not my competitors'. Piracy is just another way of boosting market share.*[Schneier]
>
> *Microsoft had exactly this in mind when they made a big push to get their products translated into Chinese and distributed across that country. They knew they would be pirated; they knew that they would make less than one sale for every ten copies used. Microsoft's Steve Ballmer has been quoted as saying: "If you're going to get pirated, you want them to pirate your stuff, not your competitors' stuff. In*

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

developing countries, it is important to have a high share of the piracy software." When China enters the free world, they will already be Microsoft compatible. Until then, Microsoft isn't losing anything. It's a perceptive business strategy. [Schneier]

Next Steps (If Ya Really Gotta Have It)

Since DRM is a new and rapidly evolving technology, organizations are encouraged to exercise diligence in evaluating providers and offerings. The standard caveats apply, look for: 1) stability; 2) reference sites of technological leadership in the industry; and, 3) user/partner recommendations. Coincidentally, the three solution providers listed previously (ContentGuard, IBM, and Reciprocal) appear positioned to meet these criteria. [Noakes-Fry, October 2000]

While outsourcing may provide "instant gratification", these solutions may not be as flexible as other options [Noakes-Fry, October 2000]. To ensure a fit with business needs, organizations seeking to adopt DRM should consider the following points adapted from Gartner Group:

1) Content type(s) to be controlled
2) The value of the content (to both the provider and recipients) against the cost of content protection
3) Life cycle of the content types to be controlled
4) Rights to be controlled (the particular set of rights for each type of content may vary)
5) Identification of technology limitations in distributor and consumer hardware and software that may impact ability of the DRM solution to function on playback devices
6) The level of trust that that can be assumed on the part of recipients
7) Solution transparency (the more transparent the solution, the less likely it is that illegal use or copying will take place and the less likely that the consumer will become discouraged and abandon the transaction)

adapted from: [Noakes-Fry, October 2000]

LIST OF REFERENCES

The following resources were used in developing this paper.

<u>books</u>

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1) [Schneier] Schneier, Bruce, **Secrets and Lies**, Wiley Computer Publishing, New York, 2000, pp. 248-253.

research services

2) [Weintraub, 2001] Gartner Group, "Content Management Providers: Timetable Toward DRM," M-13-7071, A. Weintraub, 3 July 2001

3) [Noakes-Fry, October 2000] Gartner Group, "Content Protection Through Digital Rights Management (DRM): Perspective," DPRO-93479 , Kristen Noakes-Fry, 16 October 2000

4) [Noakes-Fry, January 2001] Gartner Group, "Reciprocal Inc. Digital Rights Management (DRM) Service", Kristen Noakes-Fry and Trude Diamond, DPRO-95092, 9 January 2001

web sites - miscellaneous

5) [Amis, 2001] "Digital Rights Management Revisited," Dave Amis, 08-Apr-2001, http://www.netfreedom.org/news.asp?item=152

6) [Adobe, DRM] "How DRM Works", Adobe, http://publishing.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.adobe.com%2Fepaper%2Ffeatures%2Fdrm%2Fmain.html

7) [Dailynews, 2001] "Metallica, Dre Settle with Napster", 13 Jul 2001, http://dailynews.yahoo.com/h/ap/20010713/en/metallica_dre_napster_3.html

8) Internet Freedom, http://www.netfreedom.org/

9) [Intertrust] InterTrust, "What is Digital Rights Management?", http://www.intertrust.com/main/metatrust/whatsdrm.html

10) [McGarvey, 2001] MIT Technology Review, "Digital Rights Management," Robert McGarvey, Jan/Feb 2001, http://www.technologyreview.com/magazine/jan01/tr10_singh.asp

11) [Oasis] Oasis News, "OASIS Forms Technical Committee to Standardize Security Access Control with XML", 24 April 2001, http://www.oasis-open.org/news/oasis_news_04_24_01.shtml

web sites – standards bodies

12) Digital Property Rights Language (DPRL), http://xml.coverpages.org/dprl.html

13) Electronic Book Exchange (EBX) Working Group, http://www.ebxwg.org/

14) Extensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

15) Extensible Rights Markup Language (XrML), http://www.xrml.org/

16) MPEG Rights Expression Language , http://www.cselt.it/mpeg/

17) Open Digital Rights Language (ODRL), http://odrl.net/

18) Open eBook Forum (OeBF), http://www.openebook.org/

19) Secure Digital Music Initiative (SDMI), http://www.sdmi.org/

20) XML Cover Pages, http://xml.coverpages.org/sgml-xml.html

web sites - vendors

21) Adobe, http://www.adobe.com

22) Authentica, http://www.authentica.com/

23) ContentGuard (a Xerox, Microsoft joint venture), http://www.contentguard.com/

24) IBM Content Manager, http://www-4.ibm.com/software/data/cm/index.html

25) IBM Electronic Media Management System (EMMS), http://www-4.ibm.com/software/is/emms/library.html

26) InterTrust, http://www.intertrust.com/

27) Reciprocal Inc., http://www.reciprocal.com/

28) TrustData Solutions (formerly ASPSecure), http://www.aspsecure.com/

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced