# Global Information Assurance Certification Paper

Matthew A. Lynn
GSEC Practical Requirement (v.1.2f)(August 2001)
The Digital Millennium Copyright Act and Its Implications Toward Computer and Software Security
December 13, 2001

The Digital Millennium Copyright Act (DMCA), a recent update to the United States copyright code, is either a long-needed form of protection for the creation of novel works or an unconstitutional limitation on the ability to store and to distribute such items. This act, which was signed into law in 1998 by President Clinton, provides a legal framework for the digital creation, use, and manipulation of original material, such as software code, written material (e.g., newspapers and novels), and digital forms of music, literature, and movies. The ability to generate and to transmit identical copies of such works easily across networked computer systems has caused concern among copyright holders that they may not be properly compensated for their efforts. Although software designers have employed various methods of protection, such as hardware dongles, digital watermarking, encryption, passwords and key codes in an effort to restrict how copies can be made of their products, it still remains somewhat easy to copy and distribute most of these items via the Internet, writeable CDs, and external hard drives. Therefore, the DMCA was created to establish a protocol for how such copies can be made, where they can be used, how they can be transmitted, and how users must interact with any security measures that have been implemented to prevent any unauthorized duplication of such material. Perhaps it is this last function of the DMCA, the legal rights and ramifications concerning a user's ability to inspect and circumvent any electronic measures that copyright holders have used to protect their original works that has brought the most attention to this recent piece of legislation. A number of high-profile cases, including the arrest of a foreign software designer, the creation and distribution of code designed to allow the viewing of a DVD under the Linux operating system, and the alleged intimidation of an academic researcher, software designers, and security experts have led to the creation of anti-DMCA websites, the boycott of a major software developer, and renewed debates surrounding the free-speech rights of anyone who uses a digital form of a unique work. Nevertheless, all of these issues and events essentially pertain to a single issue: a copyright holder's ability to keep works secure in an age of proliferating digital copying. This discussion therefore will focus on the various computer and software security issues that the enactment of the Digital Millenium Copyright Act has generated.

**Legislative Background**

The most contentious portions of the DMCA are arguably those that pertain to the copying of works that have somehow been protected by a digital means of security. The reason for the enactment of the DMCA was originally to bring the United States legal code into conformity with a World Intellectual Property Organization (WIPO) treaty, which required that states that were party to this agreement provide for legislation that rendered the subversion of copy-protection measures illegal.[1] The treaty was ostensibly written to prevent the widespread copying and distribution of an author's works without appropriate compensation. However, the actual wording of the DMCA [2] criminalizes any attempt to circumvent methods that are used

to restrict access to a copyrighted work regardless of whether or not an attempt is being made to make an unauthorized duplicate of the work:

> Section 1201: Circumvention of Copyright Protection Systems
> "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that is primarily designed or produced for the purpose of [descrambling a scrambled work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or impairing a technological measure] that effectively controls access to a work [without the authority of the copyright holder]."

There are exemptions to this code, however, that allow non-profit libraries, archives, and schools to "gain access to a commercially exploited copyrighted work" for only so long as is required for the institution to decide whether or not it should obtain a copy of the work if it is not "reasonably available in another form." Another exception, which has more significant ramifications for the active protection of access-restricted code, pertains to how users can subvert any measures that software producers have employed to secure their product. The DMCA allows anyone who has

> "lawfully obtained the right to use a copy of a computer program" to "circumvent a technological measure that … controls access to a … program for the sole purpose of … analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs … to the extent any such acts of identification and analysis do not constitute infringement under this title."

Academic and other researchers are also allowed to probe the encryption used to protect such works, provided that these activities are "conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products" and that "the person has lawfully obtained the encrypted copy …, that such [an] act is necessary to conduct such encryption research, … [and] that the person has made a good faith effort to obtain authorization before the circumvention …" As with any legal wording, a number of problems can be seen to arise from how the law is crafted. The problem with the DMCA, according to one legal analyst [3] is that is not clear from the legal code what constitutes a "good faith effort." Further, it is entirely possible that a researcher could seek permission from a copyright holder who could then flatly deny that person's request, thereby quashing any attempt at encryption research. In a general sense, a software manufacturer may be able to control in the short term any examination of the weaknesses in a given piece of code, but such a stance only pertains to those researchers who follow the appropriate legal channels to do so. Further, such wording assumes that a software developer is willing to accept public knowledge of any flaws that are discovered in the means by which a piece of code is protected. Should vulnerabilities be discovered in such code, a software company might choose to bring a lawsuit against a researcher to prevent these findings from becoming public. The probable result, as has indeed already been shown to be the case, is that researchers, especially those without the ability to pay for legal research or representation, can be intimidated into not examining pieces of commercial code.

**History of Legal Cases and Other DMCA-Related Incidents**

The first well-known test of the DMCA concerned the breaking of the code (Content Scrambling System, or CSS) used to protect DVDs from being played without a CSS-enabled video player.[1] The case (Universal City Studios v. Reimerdes [4]) involved the posting of the DeCSS program on the Internet by a Norwegian teenager, the subsequent posting of the code on other websites (dvd-copy.com, operated by Shawn Reimerdes, and krackdown.com and escape.com, operated by Roman Kazan), and the hyperlink that was made to his site by an online hacker website.[5] In a lawsuit filed by the Motion Picture Association of America (MPAA) against the website (2600.com), the defendants argued that the encryption method that was used to safeguard DVD information was too weak to be an effective means of controlling access to the copyrighted material and therefore did not violate the DMCA.[6] They also argued that the program was intended to be used only to allow DVD movies that had been legally purchased to be displayed on a computer using the Linux operating system for which no MPAA-approved DVD-playing software was available. The presiding judge, however, decided that the DeCSS program was indeed a method of subverting the access control that had been designed into DVDs, that the intent of the DeCSS designer was irrelevant to the case, and that there had been no effort to obtain permission from the DVD copyright owner to perform work toward defeating the access control restrictions that had been encoded into the disc. Further, the judge determined that the online magazine was at fault because it provided a means for obtaining the DeCSS program; the hyperlink allowed visitors to the site to find the software, which meant that the site was aiding in the "trafficking" of a program that was subverting the CSS access control method.

In a separate case, the only person to have been arrested for allegedly violating the DMCA is a Russian software developer that wrote and offered for sale a program that allowed users of Adobe's eBook software to defeat the access restrictions that were included in the code. Dmitry Sklyarov's software thus allowed users to copy books, to transfer them to other computers, and to have the text be read aloud by the computer. Because of the terms of the DMCA, all of these actions were forbidden because of the access restrictions that Adobe had placed on its software.[7] Adobe's eBooks are basically secured PDF files in which selected portions of the body of the file have been encrypted.[8] Plug-ins called "security handlers" are used to enforce the encryption and key management features of these files. However, if an attacker is able to determine the document encryption key by obtaining a user or owner key, the document can be converted into an unprotected PDF file that can be viewed with Adobe's Acrobat Reader software on any computer. Even if the user's password is not known, a brute-force attack can be used to defeat the RC4 encryption. Such an effort may take only a few hours on "well-equipped workstations."[8] Sklyarov's distribution and offering of his work for sale was sufficient cause for Adobe to request that the FBI arrest the computer programmer at a Defcon-9 conference in Las Vegas in July, 2001.[3] Sklyarov has subsequently been indicted by a grand jury and is awaiting trial on these charges.

Another high-profile DMCA-related battle involves the research of Edward Felton, a computer science professor at Princeton University. In September 2000, the Secure Digital Music Initiative (SDMI), a group that represents the recording industry and electronics companies, announced that it was sponsoring a challenge for interested parties to try to remove various watermark protections in a digital music recording without degrading the quality of the

recording.[9] Dr. Felten and his coworkers subsequently claimed that they had been able to subvert the access protections in all of the watermarked pieces. However, they decided not to participate further in the challenge because they would not have been able to present their work in an academic setting due to a nondisclosure agreement that SDMI required participants to sign. The Recording Industry Association of America (RIAA) threatened to sue Felton if he made his findings public. The issue at hand was whether the presenting and publishing of information that pertained to access-control measures was protected by free speech rights or was tantamount to helping other people to defeat these software-encoded restrictions.[3] Referring to the Reimerdes case, Felton said that the judge's opinion suggested that even a text-based description of a vulnerability in a software-encoded access-control measure could be deemed a "circumvention device." Felton counter sued, the SDMI dropped their suit with the requirement that Felton could only present his findings at a Usenix symposium, and Felton's counter suit has recently been thrown out.[10]

Several other security-related incidents have come to light in the wake of these three high-profile cases. The first involves the circumventing of the security rule built into Microsoft's eBook code that prevents a book from being accessed on no more than two devices. The author of the decryption software remains to be identified and has not released the program for fear of legal action.[11] Other computer security specialists have also performed acts of self-censorship for fear of becoming embroiled in a DMCA-related lawsuit.[12] Fred Cohen, author of the evidence-gathering package Forensix, has removed this software from his website citing DMCA-related concerns about his distribution of "certain digital forensic capabilities unless explicitly funded by Law Enforcement." [13] Niels Ferguson, who discovered a "major flaw" in Intel's High-bandwidth Digital Content Protection (HDCP) scheme, has refused to publish his findings, citing that he "cannot afford to be sued or prosecuted in the U.S." because he would "go bankrupt paying for [his] lawyers." [12] According to Ferguson, the HDCP master key can be cracked "in about two weeks using four computers and 50 HDCP displays. Once you know the master key, you can decrypt any movie …"[3] Alan Cox, who controls the 2.2 version of the Linux kernel, has announced that details about security fixes in an update to this kernel would not be divulged to American users of the software. Although the details of this reasoning are rather vague, Cox has suggested that security features in the Linux operating system might be used for "rights management of copyrighted work." [14] Presumably, Cox believes that his open-source code could be used by a company to protect its own code. The further distribution of the Linux code might then be construed as providing information about that company's access-restriction technology, opening Cox to legal liability under the DMCA. Alternatively, Cox may feel that there are portions of the Linux 2.2 kernel that aid in the subversion of access-restriction code. Nonetheless, Cox feels that it is currently better not to divulge the particulars of certain changes to the Linux kernel than to open himself to possible legal action.

A final note in the current legislative saga of computer security regards the possible enactment of the Security Systems Standards and Certification Act (SSSCA), which has been sponsored by Senators Hollings and Stevens. The proposed legislation would require the embedding of copy-protection controls in almost all computers and electronic devices and would render the creation or selling of any equipment that "does not include and utilize certified security technologies" a civil offense.[15] Whereas the DMCA deals with access control restrictions from a software point-of-view, the SSSCA would presumably deal with the issue

from a hardware perspective. With the hardware changes that the SSSCA might require, it could be more difficult to gain access to security-related information that was stored in RAM or that was somehow encoded on a computer's hard drive. On the other hand, companies could be more assured that their products, such as digital copies of music or books, were only being used ("fair use" arguments aside) on the particular device for which they have been paid for and licensed. The current fate of this legislation, however, is unknown. A draft of the SSSCA was released during summer 2001, but it has yet to be introduced as a bill.

**Discussion**

A whole host of arguments have been made, both for and against, the enactment of the Digital Millenium Copyright Act, many of which deal with free speech and fair use issues. However, until the details of how the law is to be enforced are hammered out through judicial and legislative action, there are security-related issues that are of concern. These matters range from social implications of the legislation to the actual particulars of how the law is enforced under certain circumstances. These various scenarios are the subject of the following discussion.

Already a point of concern following the Sklyarov and Felton cases is the degree to which computer security professionals feel threatened by the penalties imposed by the DMCA. Although there is no data to prove such a point, it is conceivable that security researchers on the whole would rather focus their efforts elsewhere than to study the security tools that are used by companies to protect their products, thereby slowing the advance of computer security-related research. From the point of view of the corporations, however, such continued research may be of little value to them considering that the benefits of pouring money into the development of more sophisticated access control codes are marginal given that the code will almost surely be broken anyway. Plus, with the weight of the DMCA-enacted punishments on their side, these corporations might be banking that the widespread release of tools that can be used to defeat such security mechanisms is less likely, given that small-time hackers would be much less willing to risk being caught for distributing such code. The point therefore is that the DMCA may be seen from a social aspect to have some effect on the progress that security researchers may be able to make regarding a commercial need for and use of access-restricting code. However, with the plethora of open source and non-commercial related security issues that are available for study, the impact of this point of concern is expected to be minor. The fear, though, with open-source systems is that commercial software writers would only focus their efforts on a more prevalent operating system. Software that included access restrictions could then not be used with an open-source operating system and if too much software were written as such, interest in operating systems like Linux might flounder. In the worst case, development of commercial security code would be monopolized by development of a single given operating system.

From the point of view of media and other software-producing companies, the DMCA acts to enhance the security of their products in a way that no piece of code can. Through the legislation of rather harsh penalties, the weight of law stands on the side of the music recording industry, DVD publishers, computer application designers, and the like to enforce the access restrictions that they desire to implement into their code. Given the large amount of money that music recording companies certainly lost during the heyday of the MP3-swapping mechanisms

of the past few years owing to the lack of access restrictions on CDs, media-producing companies may take some assurance in the fact that although they may not have the strongest of protection technologies encoded into their products, the DMCA is in the end probably a more effective deterrent to unauthorized access to their products.

A more pressing issue, however, is how companies use their newfound legal protection in constructing code. Some software companies presumably would be interested in obtaining as much information (including a user's personal documents, credit card information, types and amounts of music and video files, tax records, and the like) from a computer as possible.[3] A malicious software writer might hide tools that gather this sort of information behind software-encoded access restrictions. If a security analyst or encryption researcher were to ask the company for permission to inspect the code by subverting the access restrictions, the company could deny permission. If researchers were to analyze the code despite the denial from the company, they might be found to be in violation of the DMCA. Thus, computer users could never be truly sure how secure their personal files were and which program they had installed on their own computer might be revealing personal information to corporate or other entities.

**Conclusion**

The Digital Millenium Copyright Act, which is a recent update to the United States copyright code, has drastically changed how copyright holders are protected in this age of digital content. Subverting access restriction measures that have been encoded into digital media or even discussing how to do so is now punishable by severe penalties. Court cases have already been brought against several people and others have claimed to have been intimidated by corporate entities or have censored their work for fear of reprisals under the DMCA. The act gives more assurance to copyright holders that exact copies of their works will most likely not be distributed widely via computer networks. That is, their products and income might be more secure than before the enactment of the DMCA, but security professionals and computer programmers are wary that the DMCA may be used against them to prevent them from examining the techniques that are being used to access-protect certain media, from writing software that enables such media to be accessed on non-supported platforms, and from assuring that access-protected code does not surreptitiously divulge private information about its users.

**References**


[1] Pfaffenberger, Bryan, "Linux and DeCSS: What the MPAA is Really After" Linux Journal. February 4, 2000.
http://www.linuxjournal.com/article.php?sid=5072

[2] Digital Millenium Copyright Act
http://www.planetpdf.com/mainpage.asp?WebPageID=1534

[3] Landau, Michael, "The DMCA's Chilling Effect on Encryption Research" gigalaw.com.
http://www.gigalaw.com/articles/2001/landau-2001-09-p1.html

[4] http://www.cs.princeton.edu/courses/archive/spr01/frs136/dvd/dvd-mpaa-3-mo.htm

[5] Wyrick, Ben, "Report on Course: The Impact of Public Policy on Computer Graphics" SIGGRAPH. August 12, 2001.
http://www.siggraph.org/conferences/reports/s2001/tech/crs1.html

[6] Weiland, Mick, "A Review of the Digital Millenium Copyright Act in Its First Application Against Decryption Software"
http://gsulaw.gsu.edu/lawand/papers/fa00/weiland/

[7] Ross, Rachel, "Copyright: What's Right?" thestar.com. September 10, 2001.
http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1000073417176&call_page=TS_@Biz&call_pageid=971794782442&call_pagepath=Business/@Biz

[8] Bailey, Daniel V. "Inside eBook Security" Dr. Dobb's Journal. November, 2001.
http://www.ddj.com/documents/s=1487/ddj0111d/0111d.htm

[9] Olsen, Florence "Legal Concerns Delay Publication of Research on 'Digital Watermarks'" The Chronicle of Higher Education. January 15, 2001.
http://chronicle.merit.edu/free/2001/01/2001011501t.htm

[10] Pruitt, Scarlet "Courts Side with Copyright Holders in DMCA Battles" cnn.com. November 30, 2001.
http://www.cnn.com/2001/TECH/industry/11/30/dmca.appeal.idg/index.html

[11] Roush, Wade "Breaking Microsoft's e-Book Code" Technology Review. November 2001.
http://www.technologyreview.com/magazine/nov01/innovation1.asp

[12] Lemos, Robert "Seccurity Experts Protest Copyright Act" ZDNet News. September 6, 2001.
http://www.zdnet.com/zdnn/stories/news/0,4586,5096701,00.html

[13] http://all.net

[14] Poulsen, Kevin "Linux Update Withholds Security Details" SecurityFocus. October 25, 2001.
http://www.securityfocus.com/news/274

[15] McCullagh, Declan "New Copyright Bill Heading to DC" Wired News. September 7, 2001.
http://www.wired.com/news/politics/0,1283,46655,00.html