My views on how programs that decrypt DVD movies for playback should be exempt from the Digital Millenium Copyright Act.

By Steven Schveighoffer

Recently in the news, I have been reading about a software utility that has the ability to circumvent the encryption installed on all DVD disks. This utility was created for the purpose of allowing users of the Linux operating system to play DVD movies on their home computers (See Ref 1). Currently, no commercial company is building an authorized Linux DVD player that I am aware of, and therefore, users of DVD-enabled computers that choose to use the Linux operating system are prevented from viewing any DVD movies that they might buy. The Motion Picture Association of America and the DVD Copy Control Authority is suing web sites for posting this utility (See Ref 2). They are using as their argument the Digital Millenium Copyright Act. I belive DVD's are exempt from this act and my argument is as follows:

In addition to not having the ability to play legally purchased DVDs on DVD-enabled hardware, it is impossible for a normal user to make an archival copy for non-profit use of the content on a DVD disk (a well established right) without first decrypting the information on it for three reasons:

1. DVD writable disks on the market today do not allow the writing of encryption keys into the disk (See Ref 3). Therefore, making a copy of one disk to another will not allow the archive disk to be viewed, rendering it useless.

2. Making a copy of the encrypted data to any other media such as a hard drive, does not allow the viewing of that data unless it is first decrypted.

3. The DVD format is a new technology that surpasses all previous ones. Since previous technologies cannot contain the same content as a DVD disk can, it is impossible to get the same content on another media. For example, DVD disks can contain multiple camera angles, multiple soundtracks, and voice overs on movies that can be switched on the fly. Also, most DVD disks contain some software that allows the user of the disk to interact with the disk. While these could possibly be generated on multiple instances of other media types (e.g. one VHS tape for each combination of soundtrack and camera angle, CD rom for interactive component), this format is not currently being offered. In addition, the combination of all the elements as a whole is what makes DVD so enjoyable, and it is impossible to copy this experience onto another media.

As a copy protection scheme, the encryption used for DVD disks is extremely weak (See Refs 4 and 5). It uses an encryption scheme that can be broken relatively quickly. Not only that, but decryption software isn't even necessary for the illegal copying of DVD disks. It is reported that certain

programs can be designed to act as MPEG card drivers and audio drivers, and they can simply output their data to a hard drive or other media after the DVD-Rom device decrypts the data (See Ref 1). In addition, a criminal can potentially obtain both DVD disks that have a writable key sector AND a machine that can write to them. If this is obtained, all the criminal needs is a source disk and he can copy the DVD verbatim to the destination disk. No decryption is necessary! Therefore, the copy protection scheme fails in several points.

It has been argued that a certain software program called DeCSS (and in effect any DVD decryption software) has little value other than to illegally copy DVD disks. This is untrue for several reasons:

1. For OS's that do not support DVD decryption devices, DeCSS allows playback of legally purchased DVD movies (in fact, that is what it was specifically designed for, see Ref 1). Without software that decrypts the data, DVD playback would not be possible on OS's such as Linux, FreeBSD, Most Unix variants, and BeOS. Since these operating systems are used by a large group of people, it offers proof that DeCSS has great legitimate value to these OS users. In addition banning DeCSS restricts the freedom of choice for people who want to play DVD's on their DVD-enabled computer. They must choose an operating system that has paid the DVD CCA for the rights to the decryption algorithm.

2. The program can be used to view legally purchased DVD disks and to make legal archival copies of disks, and to average users who cannot do either of these without DeCSS, it has significant legitimate value.

In addition, DeCSS is a combination of MPEG-2 parsing software (which is available for free without restriction), and an encryption algorithm. This encryption algorithm is not patented, and was not obtained through illegal methods. Therefore the algorithm itself should not be restricted. Therefore, this program constitutes a legally developed piece of software, and banning its legal use is to control the freedom of speech rights of its developers, and the rights of the potential users.

By virtue of these facts, the DeCSS utility has significant value besides the illegal use of it to perform copyright enfringement.

>From the facts in this letter, we can determine that:

1. Since decryption software isn't necessary to make copies of DVD's, the CSS encryption scheme used on DVDs is NOT an effective copy protection scheme.

2. The content on DVD's is not readily available in any other format, necessitating the ability to make archival copies of legally purchased DVD

disks

3. The utility that was written to decrypt the DVD content (DeCSS), or any other software that is similar, can have a significant purpose besides the illegal copying of DVDs and has very good legal uses that outweigh the others.

In conclusion, I believe that restricting the use of such software would only cause harm to individuals that plan to legally use a DVD system. Criminals who plan to infringe on copyright owner's rights will do so regardless of the existance of DVD decryption software, making the Content Scrambling System an ineffective means of copy protection and excluding it from the DMCA's clauses. Not only that, but preventing distribution of decryption algorithms that decrypt DVD disks that were developed without patent infringements or trade secret infringements (by trade secret infringements, I mean use of trade secret material by an individual that has signed an agreement that he will not disclose this information) is an infringement on the authors freedom of speech and violates the Constitution of the United States.

If you outlaw decryption algorithms because they could possibly harm others, you might as well outlaw any sharp objects such as knives because they could possibly harm others. The crime is not committed by the tool, it is committed by the person who misuses the tool.

However, I do not condone, promote, or condone the promotion of copying of DVD's for profit or distribution, including the misuse of such software as DeCSS, and I fully respect the authors right as a copyright holder to persue those individuals.

I thank you for your time and the opportunity to express my views as an American Citizen.

Sincerely,
Steven Schveighoffer

References:
1. "Interview with Jon Johansen" Copyright 2000 LinuxWorld
http://www.linuxworld.com/linuxworld/lw-2000-01/lw-01-dvd-interview.html

2. "Case Hinges on Reverse Hack" Copyright 1994-2000 Wired Digital Inc.
http://www.wired.com/news/technology/0,1282,33311,00.html

3. "Son of DIVX: DVD Copy Control" Copyright 1995-2000 The Motley Fool
http://www.fool.com/portfolios/rulemaker/2000/rulemaker000127.htm

4. "Activist Defends DVD Hack" Copyright 2000 by ComputerWorld
http://www.computerworld.com/home/news.nsf/all/9911055dvd3

5. "Why the DVD Hack Was a Cinch" Copyright 1994-99 Wired Digital Inc.
http://www.wired.com/news/technology/0,1282,32263,00.html