Macrovision Analysis of the Recent DVD “DeCSS” Hack

(November 15, 1999)

Background

As the world’s leading provider of video copy protection solutions for fifteen years, Macrovision understands and appreciates the use of technical measures to protect copyrighted content. By its very nature, commercially attractive content is vulnerable to theft, be it by professional pirates, by unauthorized consumer copiers or by hackers. However, the Hollywood studios and Macrovision have always maintained that the primary aim of commercially implemented copy protection is to keep honest people honest.

The copy protection ecosystem for DVD video includes two fundamental elements: CSS (Content Scrambling System) and Macrovision ACP (Analog Copy Protection). The CSS system was designed to implement an encryption technology that would secure the digital video content and prevent unlicensed DVD hardware manufacturers from building devices that could play proprietary video content. The Macrovision technology was selected as the de facto standard to prevent unauthorized VCR copying of the unencrypted analog playback video. The CSS system is an encryption technology; the Macrovision system is a digital-to-analog copy protection technology.

The most recent “DeCSS” hack has involved breaking the CSS 40-bit encryption algorithm, as well as discovering the majority of the DVD manufacturer unique “keys.” The DeCSS hack has nothing to do with Macrovision’s digital-to-analog copy protection technology. Fortunately for content owners, the DeCSS hack has proven to be more difficult and complicated to use than the average consumer is willing to put up with.

Macrovision and most content owners do not anticipate any serious market effect from the most recent “DeCSS” hack because of the fact that most consumers can do little more than store one movie title at a time on their PC, unless they want to make degraded MPEG-1 video CDs from the hacked DVD video. Consumers are further thwarted from utilizing the DeCSS hack on a widespread basis because of the bandwidth limitations to be able to distribute the hacked video over the Internet, the absence of cost-effective DVD recordable devices and discs, the absence of a soft DVD player which will playback the DVD .VOB files, and the absence of truly consumer-friendly software programs to remove all forms of copy protection already deployed.

Fighting piracy is a three-pronged effort – utilizing the best copy protection technology available, developing and enacting legislative initiatives that protect the right’s holder’s copyrights, and implementing education and enforcement programs that support the laws. Macrovision’s video copy protection and computer software copy protection business groups are continuously monitoring the Internet for hack sites. Macrovision has dedicated engineering teams that are working to continuously improve the security of our copy protection technologies in anticipation of future hacks. Macrovision has continued deploying its legal and technical resources towards enforcing security and technical standards for our licensees, enforcing our contracts and technical standards with existing licensees, and enforcing our intellectual property against those who illegally employ our technology or who circumvent it. Macrovision has recently served “cease and desist” orders on US and European ISP’s that host hacker sites.

Macrovision Comments on Recent CSS Hack

Why the CSS Hack is a minimal threat to copyright owners

With regard to the recently advertised CSS Hack, what do the CSS hackers get after they decrypt the DVD content? They will get clear (unencrypted) digital video content in several files that have .VOB extension. The total of these .VOB files can range in size from 4.7 GB to over 9 GB. Today's recordable DVD discs have, at best, 2.5GB capacity (or 5.2 GB for double-sided discs); therefore direct DVD copying is unfeasible. Furthermore, since recordable DVD discs cost in the vicinity of $25-$30 per disc, there is little economic incentive for a consumer to make a DVD copy. The hackers can only store a 4.7GB DVD file in their computer's hard disk. Even with the 4.7GB recordable DVD drives that are expected to hit the market next year, the hackers will only get the linear version of the DVD movies which means no navigation capability (such as menu, chapters, interaction between chapters). The hackers would need to develop a DVD player that can play the linear DVD content**. Note that in all cases, the decrypted linear DVD content will contain Macrovision copy protection trigger bits which are used to prevent unauthorized analog VCR copies.**

Currently, there are no cost-effective methods of re-distributing the 'hacked' content – either in packaged media or Internet transmissions. Cost-effective recordable DVD hardware will not be widely available in the consumer market for another 2-3 years. Additionally, the new recordable DVD formats most likely will not be backward compatible with existing DVD players or PC-DVDs. Without recordable DVD discs, it will take multiple CD-ROMS (or other equivalent magnetic or optical storage media) to store or distribute a hacked DVD movie. If CD-ROMs are used it is likely that the consumer would have to convert the hacked DVD MPEG-2 streams to MPEG-1 video CD format, which is inferior in quality to the DVD MPEG-2 format. Transferring and/or downloading a hacked DVD movie from the Internet would take over 190 hours using a standard 56kb modem operating at maximum transfer rate, or over 10 hours using a 1 Megabit/sec ADSL line.

Why Macrovision digital-to-analog copy protection is important

The CSS hack in no way diminishes the need for effective Digital-to-Analog copy protection provided by Macrovision. There are now almost 600 million VCRs worldwide and the VCR sales continue to be robust throughout the world. Recent reports from the Consumer Electronics Manufacturers' Association (CEMA) show that for 1999, the rate of VCR sales in the U.S. is running 26% ahead of the record pace set in 1998, and there are expected to be in excess of 19 million VCRs sold in the U.S. in 1999. Almost 48% of all U.S. households have two or more VCRs. With blank videocassettes selling for well under $1.00, the VCR remains the easiest, cheapest, and most available device for consumers to make unauthorized copies for themselves, their friends, and their family.

The CSS hack does not affect the Macrovision DVD Copy Protection. As described above, CSS encryption is a totally different technology with a totally different purpose than Macrovision's DVD Digital-to-Analog Copy Protection technology. The Macrovision Copy Protection is not encrypted with CSS technology. Even though the CSS keys are hacked, the hacked movie content still contains the Macrovision Copy Protection (APS trigger bits). The APS trigger bits are set throughout the movie and would all need to be reset to entirely disable the analog copy protection.

Future watermarking/play control technologies will enhance copy protection security

Macrovision Comments on Recent CSS Hack

To counter future CSS hacking, ‘watermarking’ and ‘play control’ technologies are the true digital-to-digital copy protection solution – and one hopes that the CSS hack will expedite the pending CPTWG (Copy Protection Technical Working Group) industry-wide decision on watermarking. The Millennium Group (Macrovision, Philips, Digimarc) has proposed a robust watermarking/play control solution to the CPTWG that will address the shortcomings of the CSS encryption system.

In addition, the Digital Transmission Copy Protection (DTCP, i.e., secure 1394/USB) will help to ensure another form of copy protection by securing the transmission links between digital devices. In the future, watermarking will work in tandem with DTCP and with Macrovision’s digital-to-analog copy protection to ensure a watertight ecosystem to protect rights owners’ video content in all facets of digital and analog media, and digital and analog transmission.

Cautionary note on weakness of “remarking” watermarking approach

Macrovision believes that the CSS hack demonstrates a potential Achilles heel of the “remarking” technology that has been proposed by the Galaxy Group for ‘copy-once’ watermarking. The Millennium Group has proposed an encrypted “ticket” approach. A fundamental difference between the two competing solutions is that the remarking encoders will reside in millions of consumer devices, thereby increasing the exposure to hacking. The Millennium ticketing approach is inherently more secure since it relies on a single watermark that is encoded at the source and does not proliferate watermark encoders in all consumer devices.

Legislation and other future copyright protection technologies

By combining appropriate legislation with an industry-wide economic and secure watermark standard, the rights owners can further assure that copyright protection in the digital world will be more than adequate to “keep the honest consumer honest” and even to go a long way toward controlling professional piracy.

Other technologies that are anticipated to be available in the future and which will also assist in protecting content include CSS2, CPRM, and DVI-CP. Additional hardware and software security features that Intel and Microsoft will be embedding into microprocessors and operating systems in their future might also help to overcome CSS' shortcomings. In general, the PC security developments are being considered in the context of secure Internet communications. Macrovision intends to develop application software solutions that will work in this environment to further protect video and audio content – across as many varieties of digital media formats and distribution channels as are available.