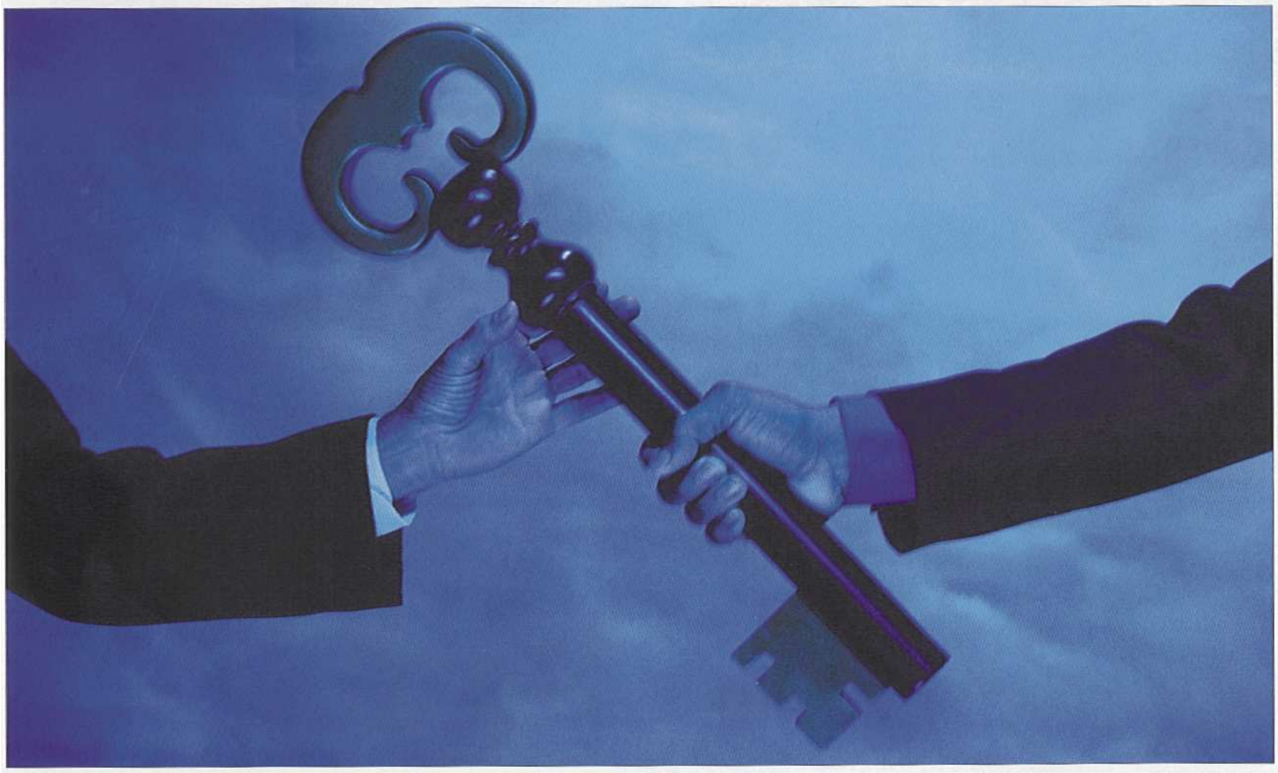


Combating piracy with copy protection solutions

The issue of copy protection is a very serious one indeed, and to help combat the rising tide of illegal downloading and copying, record companies and games publishers alike are implementing CD copy protection solutions. However, there have already been a number of widely reported problems with some copy protected CDs.

GEORGE COLE

Music companies and games publishers literally know to their cost that it's not enough to create good content, put it onto a CD and then distribute it. In an age where digital copying hardware and software is widespread, affordable and easy-to-use, content holders must use some form of copy protection technology if they are to prevent large amounts of revenue haemorrhaging through the unauthorised copying and distribution of their software. As a result, a myriad of CD audio and CD-ROM copy protection technologies are being employed and installed in mastering houses and replication plants.

Audio copy protection

Ever since the first domestic tape recorders went into homes, the music industry has been concerned about lost sales caused through the copying of tapes and discs. Those with long memories will recall the record industry's panic at the introduction of the cassette, the 'home taping is killing music' campaigns and legal moves to stop the production of double cassette decks. They may also recall the industry's successful moves to put copy control onto R-DAT, so putting another nail in that format's coffin, and the addition of the still current, but largely unused, digital-digital copy control flags on Audio CDs.

But even bigger threats are the home PC, CD burners, MP3 ripping software, cheap CD-R discs, peer-to-peer (P2P) networking and broadband Internet connections.

The IFPI, the music industry's world trade organisation, estimates that last May, there were more than 3 million people worldwide who had access to 500 million music files on the Internet, most of them illegal. "The PC industry hasn't helped us," says Cary Sherman, president of the Recording Industry Association of America (RIAA). "Home PCs are marketed as entertainment machines which come with CD burners and bundled ripper software." Meanwhile, some consumer electronic companies are aggressively promoting home CD recorders.

Today's situation is "not like home taping," says Jay Berman, chairman and CEO of IFPI. "Digital technology lets you make a perfect copy of the original, and you can then use the Internet to distribute that. It means an individual becomes an international record company." The IFPI puts a lot of blame on illegal downloading and copying for the 5% fall in global music sales by value and 6.5% by volume in 2001. And for the first time, CD sales fell by 5.1%. In some territories, CD-R discs sell for 15-20 cents each, and in countries such as Germany, CD-R sales are almost the same as sales for pre-recorded CDs.

The result has been the launch of copy-protected CDs designed to prevent consumers from playing discs on a PC. All the five major music companies – BMG, EMI, Sony, Universal and Warner – have either released copy-protected discs or are actively investigating their use. Sony Music Europe, for example, has launched more than 130 copy-protected CD titles and Jonathan Morrish, vice president of Communications, insists: "It's important that we make a stand. The rate of decline in music sales in countries like Germany is staggering." Sandra Wieflingseder, product manager for Sony DADC's key2audio CD copy protection system, says: "The music industry is afflicted by plentiful CD burning and Internet piracy which is causing enormous damage to legitimate record sales, so copy protection solutions are the logical consequence."

There are four main CD copy protection systems on the market: US company, Sunncomm, markets MediaCloq and its technology was used on the first discs to be publicly acknowledged as using copy protection technology, Charley Pride's *A Tribute To Jim Reeves*, on Music City Records.

Sony DADC's key2audio is on more than 25 million CDs in Europe and is available in all Sony plants worldwide. "Negotiations with other companies are in the final phase," says Wieflingseder.

"The technology will never be hack-proof, at best it is a deterrent which should significantly reduce the level of mass illegal copying."

Israeli company, Midbar Tech, markets Cactus Data Shield, which is now on more than 30 million discs worldwide, says the company. "Our licensing to CD plants is going well and we have plants with the system in Europe, Asia and North America, and we are looking to expand into other countries," says Noam Zur, Midbar's VP sales and marketing.

Macrovision's SafeAudio (developed in conjunction with the Israeli technology company TTR) is now licensed to 25 companies with 30 plants around the world, including Cinram, Sonopress and Disctronics, says the company.

Link Data Security's Hans Pedersen

All companies marketing CD copy protection technology says that it requires little or virtually no alteration to existing CD manufacturing equipment. In some cases, an additional encoder needs to be installed on the production line, but in others, a software upgrade to existing encoders is sufficient.

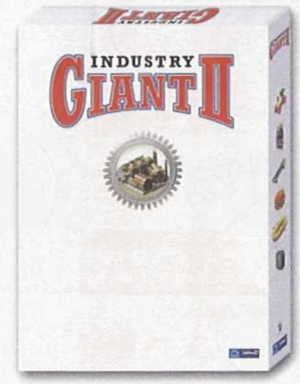
Not surprisingly, developers of CD copy protection systems are reluctant to disclose too much information about how their technology works, but all exploit the differences between the CD Red Book and CD-ROM Yellow book specifications. All the systems are designed to either stop consumers from playing audio CDs in a CD-ROM drive and/or prevent music files from being ripped and then uploaded to the Internet. Some systems, like key2audio, work by using the LBR to add a hidden digital signature to the disc during the glass master manufacturing process, which prevents a computer from copying or ripping the disc contents.

Others, like SafeAudio, add errors to the music, which audio CD players can correct but CD-ROM drives cannot. The result is that copied music files suffer from pops and clicks. Timing errors can also be introduced to the disc, which confuse a CD-ROM drive or the audio tracks may be hidden from a computer drive. The target group for all these systems is the casual copier and not the professional pirate or techno-savvy cracker or hacker, says Sarah Roberts, communications manager for the British Phonographic Industry (BPI), "The technology will never be hack-proof, at best it is a deterrent which should significantly reduce the level of mass illegal copying."

But Bill Foster, a senior consultant at the research company Understanding & Solutions, points out that: "Trying to add a new technology to a 20-year-old format is going to be problematic." One issue is compatibility with hundreds of millions of audio CD mechanisms out there, including CD players, CD recorders and CD-ROM drives. Audio CD mechanisms are also in PC CD-ROM drives, DVD players, games consoles (like PS2) and in-car systems.

There have already been a number of widely reported problems with some copy protected CDs. When BMG released Natalie Imbruglia's *White Lilies Island* (encoded with Midbar's Cactus Data Shield) in Europe last year, there were dozens of complaints that the disc would not play in some consumer CD players or CD-ROM drives. BMG was forced to reissue the disc minus Midbar's technology. There have also been complaints that these technologies can cause PCs to crash or even damage Apple Macintosh computers.

Brian McPhail, Macrovision's VP and senior manager of Consumer Software Division, says the reason SafeAudio was late entering the market (it was launched in summer 2001) was because the technology underwent rigorous testing involving hundreds of CD drives and players. "Some of the [playability] disasters we've seen were due to people getting the priorities wrong. They have produced a secure disc that is not playable. We told the music industry to wait until the playability was better." The result is that most CD copy protection systems have been enhanced or upgraded to improve playability. At this year's Midem 2002, Midbar unveiled a new version of Cactus Data Shield, which the company says, "resolves all known issues of playability encountered to date." Sony DADC says key2audio-protected discs are compatible with 'virtually every music player on the market.'



JoWood have used SecuRom on its *IG2* game

The problem of compatibility led Philips to declare that copy protected CDs did not adhere to the Red Book standard and, thus, should not be described as audio compact discs or bear the CD logo. Gary Wirtz, general manager of Philips' Copyright Office, believes that copy protection technology could cause long-term playability problems, especially systems that modify the disc's error correction system. Meanwhile, last November, the BPI notified its members of the importance of clearly labelling that copy protected CDs would not play on PCs or Macs, or music companies risk falling foul of the UK Trades Descriptions Act. In the US, court action has resulted in the strong recommendation that publishers include notification on the disc's cover exactly what copying and play limitations apply to a copy-protected CD.

The music industry has been stung by criticism that it is now preventing consumers from playing music they have legitimately purchased on a home PC, and also stopping them from porting music to portable music players like MP3 players. As a result, music companies are taking a more subtle approach to copy protection. "We encourage the industry to adopt a copy management approach rather than simple copy protection," says Pam Horowitz, president of the US National Association of Recording Merchandisers (NARM). Cary Sherman of the RIAA agrees: "The proposition used to be unlimited copying or no copying, copy protection or no copy protection, but that's a false dichotomy. We have to find a balance between allowing consumers to use music more flexibly and yet, at the same time, protect artists and music companies."

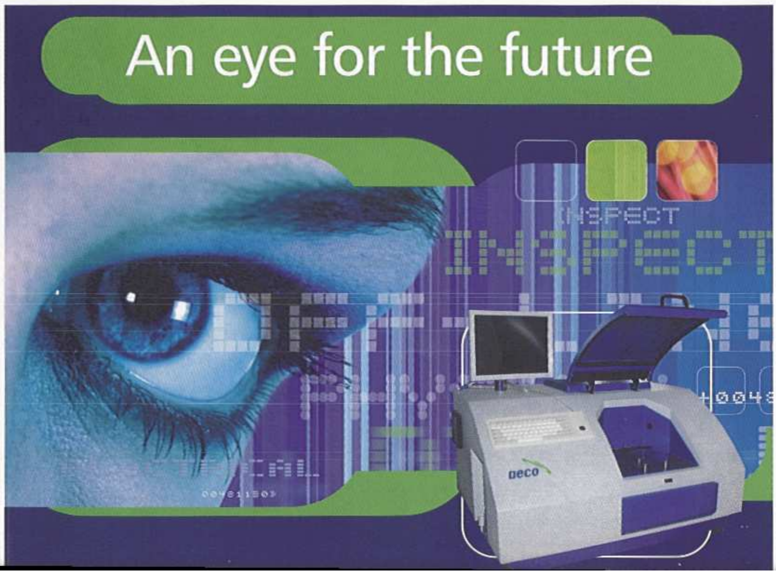
For this reason, vendors of CD copy protection technology offer their clients a suite of solutions, which includes playback on a PC. These systems are combined with digital rights management (DRM) technology that allows music companies to control how the content is to be used by consumers. Sunncomm's MediaCloq includes a system that allows owners of a legitimate CD to register the product and then download the CD music tracks as pre-ripped, DRM-protected MP3 files from the Internet. Sunncomm is also pushing its PromoPlay system, which would allow CD owners to send DRM-protected music files to a friend's computer. The DRM technology would limit the length of time or the number of playback sessions before the shared music files became unplayable.

Three versions of Cactus Data Shield are available: CDS-100 allows CDs to be played on CD players but not PCs. CDS-200 enables discs to be played on CD players and PCs, but users cannot download the music tracks on to a hard drive. CDS-300 makes it possible to download content from the Internet for playback on a portable music device. Sony DADC has introduced key2audio4pc. The latter uses a secure database that assigns each key2audio disc with a unique 9-digit serial code. The disc's owner can go to a designated website or portal, enter the serial code number and then receive the CDs music tracks as a tethered download or streaming content.

Macrovision offers various forms of SafeAudio. SafeAudio Lite is designed for long-playing discs that have no extra space. SafeAudio Balanced provides strong protection and high compatibility with CD players, says Macrovision. SafeAudio Max offers stronger protection, but is less compatible – Macrovision recommends this for small-run pressings like promotional discs sent to reviewers. SafeAudio Authenticate is an optional extra designed for playing protected multimedia content (such as music, video, text and graphics) on a PC.

"The big concern is a game getting cracked and posted on the Internet within days of being launched."

Many websites, chat rooms and bulletin boards discuss copy protected CD titles and sometimes offer hacks around them. But McPhail says: "Hacking isn't a funny subject, but we sometimes laugh at some of the hacker websites because they disseminate so much misinformation, like incorrectly identifying discs with a technology we know isn't being used." But opponents of CD copy protection technology may have the last laugh, warns Foster: "None of the systems include analogue protection, so there's nothing to stop someone from running an audio lead to a PC sound card. I doubt if many people would notice the difference in sound quality." Even so, music companies are bound to welcome anything that helps slow down the tide of illegal music files flooding on to the Internet every day.



Hacking is a major concern for content owners

PC games

Games companies are using a variety of copy protection systems because, as John Hillier, head of the anti-piracy unit at the European Leisure Software Publishers Association (ELSPA) explains, "It can take two years to develop a game and the crucial period is the first six weeks of launch when the bulk of sales are made. The big concern is a game getting cracked and posted on the Internet within days of being launched." For once, time is on the side of the content owner. Whilst any copy protection system can be cracked given time, to have a deep affect on sales, hackers will need to have cracked the protection in those first couple of months of release.

Gerhard Neuhofer, international security manager of games software developer, JoWood Productions, says: "50% of games on the market are pirated." John Metcalfe, chief executive of Pan Technology, says: "I can probably get you any software you want from the Internet in half an hour – piracy is that bad."

Many home PCs now include high-speed CD burners that are raw data burners. Anti-copy systems often place digital signatures in the sub-channel, which raw data burners can copy. Coupled with this are software tools like CloneCD, BurnWrite and DiscJuggler, which are designed to make clones of CD titles – including their digital signatures. Manufacturers of these products say they simply enable consumers to make a copy of their software and then keep the original disc safe, but their scope for misuse has not gone unnoticed by home copiers and professional pirates.

Current CD-ROM protection systems include Sony DADC's SecuRom, Macrovision's SafeDisc, Petersen New Media's Compingo and Link Data Security's CD-Cops. Many formats work by applying protection to the CD-ROM's main executable file. Typically, a digital signature is added to a CD-R gold master and then sent to the disc replicator, where it is burnt into the glass master. The CDs produced from this glass master are then assigned an access code that the user must enter when running the software (CD-Cops offers an autocode system that does this without any user intervention). The owner can only play the game when the original disc is in the CD-ROM drive. When the game is played, the EXE.file is only unlocked when the digital signature is detected. Star Force Technologies Star Force Professional 3.0 uses a different approach that ties the executable to the physical parameters of the disc. Instead of using a digital signature it uses the geometry of the glass master used to make the genuine discs. The system produces a 24-byte unique key that is used by the executable to identify a legitimate disc – copied discs will have different physical specifications.

> **"50% of games on the market are pirated. I can probably get you any software you want from the Internet in half an hour – piracy is that bad."**

Petersen New Media's format, Compingo (that's Latin for "in a safe place"), formerly known as SafeUnlock, is based on two Macrovision products, SafeDisc and SafeCast. Compingo allows software to be protected on a network and also offers a digital rights management system that allows content holders to control how their software is used. It can also be used to replace hardware-based dongles, says Clive Burling, Petersen's managing director.

He adds that while Compingo's major target audience is the business-to-business market, it could also be used by games companies: "We're talking to one games publisher who is thinking about putting ten games on to a DVD-ROM and offer consumers a try-before-you-buy service. Our system would allow the games to be played for a pre-set time period or a number of times before users would be offered to take out a subscription or buy the game on-line."

Simon Mehlman, marketing manager at Macrovision UK, adds that Compingo offers games publishers a new and fast distribution system for reaching games players: "They could deliver secure, copy-protected games straight to a home PC. For consumers, it's a convenient and secure system for buying legitimate games. There's no waiting involved – the game is sent directly to your computer."

Adding copy protection technology to games software involves additional costs like royalties, and there are issues such as compatibility. Hans Pedersen, chief executive of Link Data Security says: "Generally, the games industry prefers cheaper protection products and accepts the fact that the CD-ROMs are easily copied. Some game manufacturers focus on protection as a pure cost rather than the increased revenue it creates." But many games manufacturers do see the benefits of copy protection.

Sony DADC says the cost benefits of copy protection are highly attractive. The company says a games title costing €40 at retail, giving revenue of €4 million. Now, imagine the piracy rate is 50% (a not unreasonable estimate), which means 100,000 lost copies. If using SecuRom generates just an additional 5% of sales, that's an extra €200,000 for an outlay of less than €11,000. Little wonder that SecuRom's clients include Sierra, Eidos, Inforgrams and Disney Interactive. Macrovision says 60-70 million games discs each year use its SafeDisc technology. StarForce's system is used in the Far East and several European countries. Spokesperson Anatassia Kojermyakina says: "Games publishers are amongst our major clients."

This raid by officials uncovered pirated optical media

Sony DADC's Key2audio is available at all Sony plants

Copy protection is a cat-and-mouse game between games developers and copy protection companies pitched against hackers and crackers. Just recently, the stakes have been raised with the development of smarter copy protection technology. StarForce has introduced File Protection, which protects the data files used by the program and is ideal for multi-level games. Macrovision's Brian McPhail, says: "We're taking a multi-padlock approach so that the protection is like an onion skin. We have an API that developers can use with their own code to attach more padlocks to their product."

Sony DADC and JoWood have developed an upgrade to SecuRom that includes a Trigger function. It enables developers to add authentication points throughout a game and not just at the start-up. "You can design a game where authentication is required just before you say, shoot the aliens. If the game has been copied, there are lots of options. You can mess with the controls so that, say, the left button becomes the up button, and you can have a pop-up message informing the user that they are playing a pirated copy – you could even crash the computer," says Neuhofer. The upgraded version of SecuRom also stops programs like CloneCD from copying discs. JoWood have put the new version of SecuRom on its game *Industry Giant 2* and the company says it has not seen any copies produced from disc cloning software.

Copy protection is a cat-and-mouse game between games developers and copy protection companies pitched against hackers and crackers.

Watermarking

Watermarking involves embedding an invisible watermark into content, such as audio or video, and playing the content in a playback machine that uses detector circuits to detect whether a watermark is present or not. If the watermark is detected, the disc plays and if it isn't, the machine refuses to play. The DVD-Audio format adopted a watermark system developed by Verance, and DVD-Audio playback equipment must include watermark technology, although it is optional for software. Looking to future DVD formats and players, the DVD Copy Control Association (DVD-CCA) has been evaluating watermarking technology for DVD discs with audio/video content. Verance believes its technology could be used for protecting the audio, but faces competition from a group of companies called the VWM Group, consisting of Philips, Macrovision, DigiMarc, Sony, NEC, Pioneer and Hitachi, which has developed a rival technology.

The DVD-CCA was planning to announce its preferred technology last May, but postponed its decision for three months. However, in August, a decision had still not been made. Joe Winograd, Verance's chief technology officer, says: "Our technology is super for protecting audio content on an AV title. Our view is that the best outcome is for both technologies [Verance and VWM] to be used, although there are cost issues. The jury is still out." ■