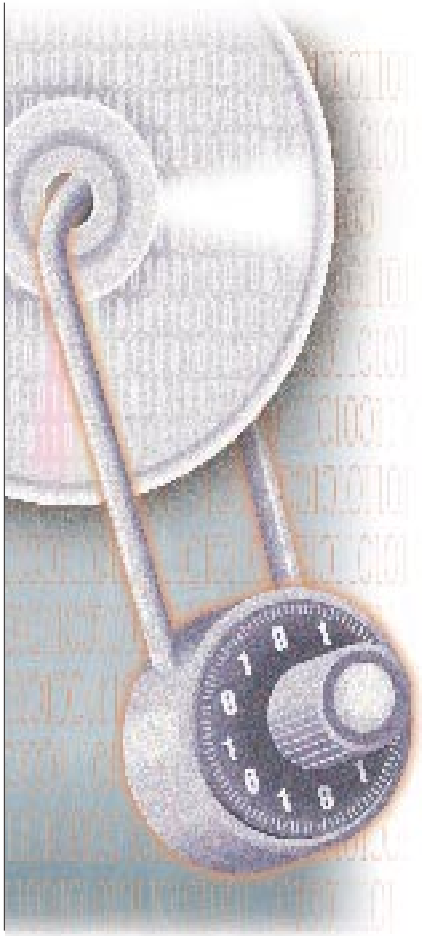


Illustration by Daniel Guidera



RAMPANT PIRACY OF UNPROTECTED DIGITAL MEDIA HAS CONTENT DEVELOPERS AND DISTRIBUTORS SCRAMBLING TO CONSTRAIN, REDEFINE, AND EXPLOIT THIS “NEW WORLD ORDER.” IN DEVELOPING YOUR MEDIA-RECORDING AND -PLAYBACK DEVICES, BEWARE OF CREEPING SECURITY ELEGANCE THAT, LEFT UNCHECKED, WILL GIVE RISE TO GADGETS NOBODY WANTS—OR CAN FIGURE OUT HOW—TO USE.

Media security thwarts temptation, permits prosecution

NUMEROUS LAWSUITS, some of which have already returned verdicts against the defendants, attempt to curtail the illegal distribution of copyright-protected digital media, such as electronic books, still images, audio files, and video movies. Rock band Metallica and rap artist Dr Dre have even taken the unusual step of pursuing legal action not only against a software company whose product supposedly promotes such content-sharing, but also against

several universities whose students swap files using the school-supplied computer networks. Consortia such as the Recording Industry Association of America (RIAA) and Motion Picture Association (MPA) are frantically developing security standards to protect their traditional revenue streams as e-stores replace brick-and-mortar and as electrons replace paper, plastic, magnetic tape, and silver-halide film. What’s all the fuss about?

Napster, which lets Internet-connected users view and download MP3 files stored on other computers, boasts millions of registered users and claims that

because its servers don’t host the files, it’s not responsible for illegal use of its software. Gnutella is a similar program developed by Justin Frankel, the originator of the popular Nullsoft WinAmp MP3 player. Gnutella extends access and exchange to any type of file (including, unfortunately, pornography); uses a direct peer-to-peer network connection instead of a central director server; was released in open source this spring (to the consternation of Nullsoft’s purchaser, America Online); and has spread throughout the Internet in dozens of mutations. Scour.net’s Scour Exchange and programs such as CuteMX, FreeNet, iMesh,

At a glance 102
Back to basics..... 104
Belatedly closing
Pandora’s box 106
Securing—and circumventing—at high speed 108
For more information 116

and VBGnutella offer similar features. College students, who historically purchase a significant percentage of audio CDs and videotapes, have enjoyed speedy broadband Internet access for years, thanks to their university accounts. With ADSL (asymmetrical-digital-subscriber-line) and cable modems now entering homes in a big way, even more traditional music and video consumers can quickly download and stream multimegabyte files.

Where are these files coming from? Today's high-powered PCs can achieve bit-accurate extraction of CD audio content and compress it to one-twelfth (MP3) or even one-twenty-fourth (MS Audio) its original size with little-to-no discernible quality loss (**Reference 1**). Both extraction and compression occur several times faster than ordinary playback speeds, and digital copies retain much higher quality than bootlegs made in the analog past. Multigigabyte hard drives are now pervasive, as are fast-writing CD-recordable drives. Rapid encoding and transcoding of video streams are now within the reach of computer users. Courtesy of programs such as DeCSS, a transcoded

AT A GLANCE

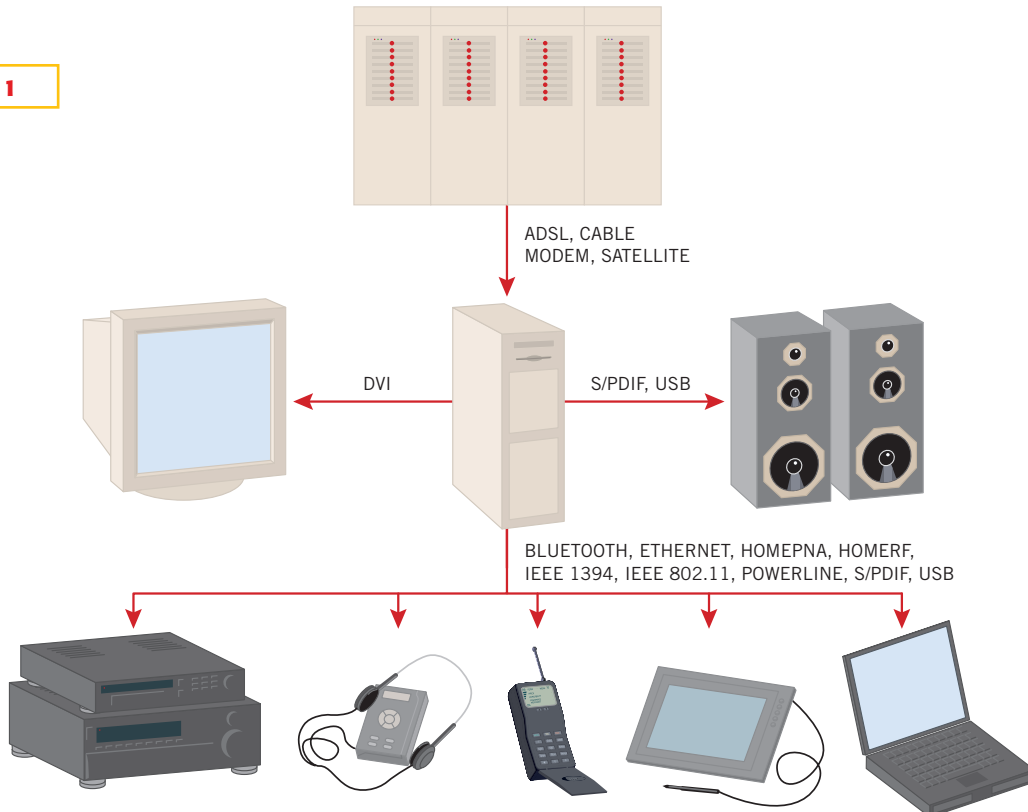
- ▷ Burgeoning digital text, audio, and video media combine with high-speed Internet access, high-performance computers, and cheaper and denser storage to create a piracy potential that gives Hollywood nightmares.
- ▷ When evaluating security algorithms for incorporation within your systems, be sure to balance robustness with ease of use and performance.
- ▷ Don't let the content developers' and distributors' fear and greed lead you to implement features that circumvent privacy or restrictions that violate consumers' duplication and transfer rights for their legally obtained media.
- ▷ An ideal security system combines the concepts of authentication, encryption, and renewability.

DVD, albeit with some audio- and video-quality loss, can fit onto a CD. Large-screen, high-resolution computer monitors can easily display high-definition

images, portable MP3 and MiniDisc players are obsoleting analog tape, and digital speakers and high-definition-TV displays are establishing footholds in homes.

In attempting to stem the flood of illegal media sharing, the content creators and distributors and you, their equipment-manufacturer partners, must walk a thin line. On the one hand, you're enforcing the valid copyright claims of those who developed the material. However, you can't excessively constrain customers who are exercising their legal rights to make copies for their own use of media they own and to transfer ownership of that purchased media to others. Media-security, or DRM (digital-rights-management) systems should be invisible to honest users (this invisibility is called "eliminating false positives"), while acting as strong deterrents to pirates. And, to simplify your implementation, one or only a few DRM systems are desirable, though recent trends point to an explosion of alternatives. The IEC (International Electrotechnical Commission) is attempting to standardize a means of coping with this diversity of op-

Figure 1



High-speed digital interconnections both to and within homes transform into reality *The Jetsons* creators' cartoon vision of the future, but they also raise serious security concerns.

BACK TO BASICS

People often use the terms “encryption” and “watermarking” interchangeably. In truth, the terms refer to different technologies, although both are important aspects of a comprehensive digital-rights-management system, and you can sometimes use watermarking to implement encryption.

Two main types of encryption exist. Symmetrical, or synchronous, encryption uses the same security key to “lock” and scramble an outgoing file and to recover a bit-exact copy of the original content at the destination. Examples of symmetrical encryption include the now-broken DES (Data Encryption Standard); its interim replacement, triple-DES, which, as the name implies, runs each data packet through DES encryption three times; next-generation AES (Advanced Encryption Standard); and RC (Rivest’s Cipher). The primary advantage of symmetrical encryption is its high

speed encoding and decoding, which occurs because the algorithms employ relatively simple transposition and substitution steps. The Achilles’ heel of the approach, though, is the common key, which the source must transmit to the destination via a secure channel or a trusted third party. If something intercepts the bit stream and the unintended recipient figures out the key, the media is vulnerable. On the other hand, clever encryption can result in the delivery of a legitimate-appearing but incorrect piece of media, such as a bogus memo, to a recipient using an invalid key.

Asymmetric, or asynchronous, encryption employs dual keys (**Figure A**). The sender encrypts the media with the recipient’s public key, and the recipient decrypts it with his or her private key. Exchange of public keys requires no secure channel, and the recipient can ensure authentication of a valid sender. However,

the key-generation, encryption, and decryption algorithms, commonly based on prime-number techniques, require multiplication operations that are time-consuming and performance-intensive. Asymmetric encryption examples include the RSA (Rivest, Shamir, and Adelman) and Diffie-Helman algorithms.

Hybrid schemes that combine asymmetric and symmetric encryption, such as a combination of RSA and DES, are also possible. Consider, for example, the approach that HDCP (High-bandwidth Digital Copy Protection) takes. Asymmetric encryption establishes the initial authorization between host and display, as well as the periodic reauthorization. Faster symmetric compression handles the content transfer. Any performance-critical application can incorporate a similar approach. DTC (Digital Transmission Copy Protection) comprehends support for both asymmetric and symmetric protocols. It supports symmetric protocols for their supposed lower value, single- and free-copy material.

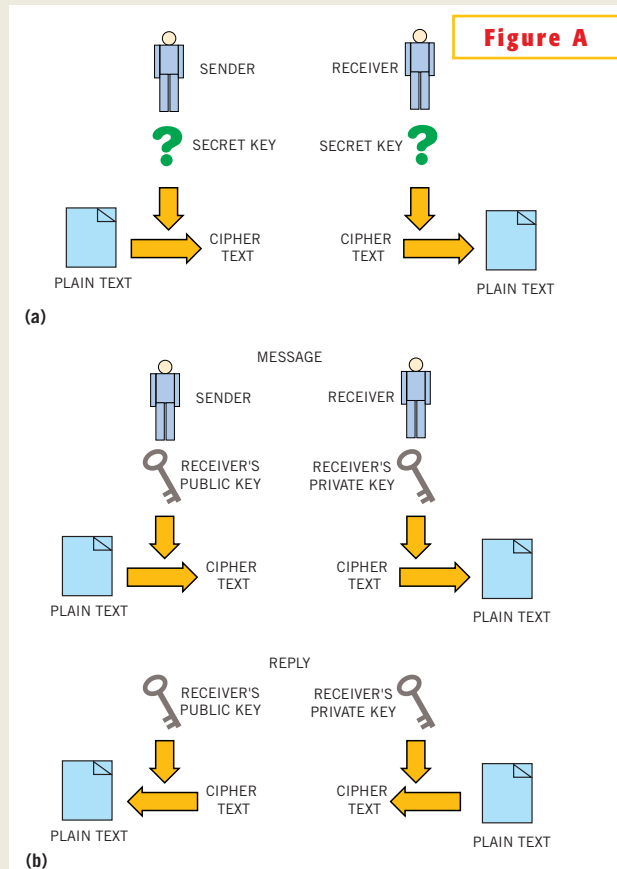
Streaming delivery is the key target of RPK SecureMedia, a New Zealand (therefore not subject to US export restrictions) cryptography company funded by, among others, streaming-media pioneer RealNetworks. RPK claims that its proprietary approach combines the benefits of public/private-key systems, such as authentication, digital signatures, certificates, and key management, with the speed of symmetric systems in one encryption and decryption engine. The Encrytonite Toolkit offers a choice of 80 levels of security using 127- to 2281-bit-long keys. Detractors point to the fact that no one knows how robust RPK’s proprietary encryption algorithms are, because they haven’t been subjected to the same intense scrutiny as standards-based alternatives, such as those from Intel spin-off PassEdge.

RPK supports a variety of platforms, including C and C++ libraries for Windows 9x and NT; HP/UX, Solaris, Linux, Java, and Delphi; DLLs (dynamically linked

libraries) and ActiveX controls; and an ANSI-standard C library for embedded systems. Tested compilers include Visual C++, Borland C++, and Gnu/g++. One other unique attribute of the Encrytonite approach is RPK’s assertion that, aside from greater initial latency analogous to a FIFO-buffer fill, increased key length does not degrade performance. The company is developing hardware-based encryption and decryption accelerators to supplement its software offerings.

PassEdge’s StreamAccess encryption algorithms take advantage of any hardware-accelerated integer arithmetic logic within a microprocessor, such as Intel’s MMX (multimedia-extensions) instruction set. The company targeted a 166-MHz Pentium CPU for its client-side security software and estimates that with a less-than-1-Mbyte memory footprint, including a graphical user interface, the device will consume no more than 3% of a 450-MHz Pentium II CPU while decrypting an incoming 1.5-Mbps stream. Note, though, that these performance claims are only for access security. Should you also want to incorporate the company’s BeyondAccess copy-protection algorithms, they’ll take up more system resources. Although most of PassEdge’s work has centered on Wintel-based systems, the company’s products don’t have operating-system-specific links, such as Windows COM calls, improving portability. Client-side software is free; PassEdge makes its money from server-side sales.

Now for watermarking, or *steganography* (from the Greek words for “covered writing”) (**Reference A**). Your first exposure to this technique may have been when you held a piece of paper up to a strong light and saw a faint, normally invisible, manufacturer or publisher logo. Digital “fingerprinting” applies the same concept to electronic media. Watermarking might find use as a means of hiding the secure key in symmetrical encryption. More commonly, however, content distributors use watermarking to encode copyright and other media



Symmetrical encryption’s key benefit is its speed (a), whereas asymmetrical encryption is more robust and offers a full set of capabilities (b).

source information, and to document usage regulations. These rules include duration of access, the number of times a user can access the media under certain purchase conditions, duplication capability (or lack thereof), and geography-based access rights (such as a movie that you can play in the United States but not in Europe). Internet search “spiders” can then use all of this embedded data to detect illegal media distribution and to subsequently prosecute the perpetrators.

Think about it for a minute, and you’ll realize how challenging watermarking is to implement. The watermark must be durable enough to withstand repeated media degradation due to transcoding (such as WAV conversion to MP3, TIFF translation to JPEG or DV encoding to MPEG). However, the watermarking must be invisible or inaudible under normal usage conditions. It can’t inject so much additional randomness into the source media that it increases the compressed file size necessary for a given quality level (or degrade the quality level at an application-defined greater file size or bit rate). It also must tolerate transmission errors; a watermark can’t be voided by dropped packets during a streaming transmission or circumvented by selective deletion of portions of a picture or sound clip.

Digimarc is perhaps the best-known image-watermarking company. Photo steganography works by slightly shifting the color values of random pixels to whose wavelengths the human eye is insensitive and therefore from which the alteration is comparatively unnoticeable. Beginning with Version 4.0 of PhotoShop, Adobe began distributing a plug-in that detects Digimarc watermarks, such as photographer copyright information, in images.

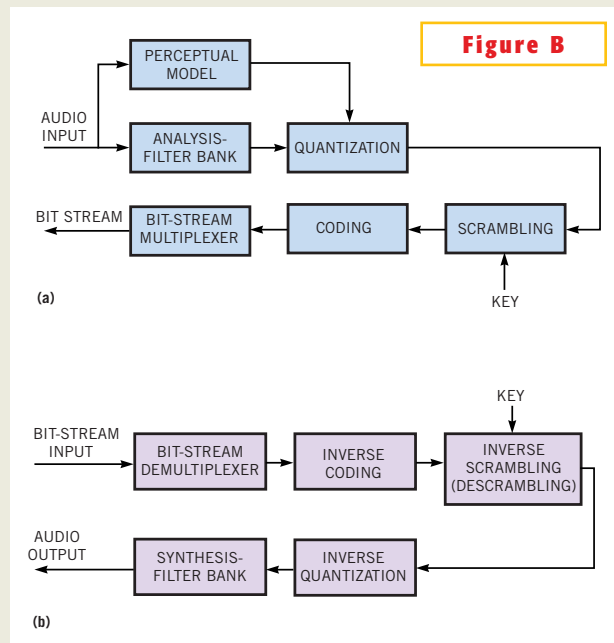
Digimarc has recently partnered with a number of PC-tethered videocamera manufacturers to distribute software, which, if you hold a magazine advertisement up to the camera, detects its watermark and sends notification to the advertiser indicating that

you’d like additional information. You could extend Digimarc’s techniques to the video domain, but frame-by-frame watermarking would probably be overkill as well as too time-consuming and expensive.

One common technique available to those wishing to watermark digital audio involves injection of low-level broadband and time-independent noise. As with still images, you need to balance transparency—the inability to hear the watermark, particularly at critical “sweet-spot” frequencies—with robustness—the ability for the watermark to withstand multiple generations of compression and transcoding. Another more sophisticated audio-watermarking approach, *echo hiding*, exploits the fact that, although reverberation itself is perceptually important, some reverberation details are perceptually irrelevant. Watermarking information hides in echo timing and amplitude data, including using physically “impossible” echoes that the human auditory system ignores.

The Fraunhofer Institute, which developed much of the technology behind the MPEG audio (most notably MP3) and newer AAC (advanced audio codec) algorithms, has also spent much time and effort on audio encryption and watermarking. The company’s watermarking approach is high-performance, which is important when companies must generate license-specific versions of media. The approach also can operate on already-compressed audio files (references B and C). It either slightly increases the bit rate to hold quality constant or partially decodes, then more aggressively quantizes and adds watermarking bits to, perceptually irrelevant frequency bands.

Fraunhofer’s encryption technique is equally interesting (references D and E). The company encrypts each group of audio samples *within* the encoding processes of spectral decomposition, temporal and frequency masking, and quantization and then descrambles before inverse quantization and filter-bank



By embedding the encryption process within the encoding algorithm (a), you can create an audio file that’s playable (at degraded quality) using any decoder and easily unlocked (b) for full fidelity reproduction (courtesy Fraunhofer Institute).

resynthesis (Figure B). Embedding encryption within encoding allows the encryption algorithm to selectively place its manipulations in certain frequency bands. This flexibility means that you can create an encrypted file that an audio decoder without access to the proper key can still play, albeit with an adjustable amount of distortion. Applying this concept to e-commerce means that a customer could preview entire songs versus today’s short clips and then purchase a key to enable access to them at their full quality.

For more information on encryption, check out references F and G. Good Web sites to continue your media-security research include Cryptography Research (www.cryptography.com), Counterpane Labs (www.counterpane.com/labs.html), and Francis Litterio’s cryptography page (world.std.com/~fran/crypto.html).

REFERENCES

- A. Jajodia, Sushil, and Neil F Johnson, “Exploring steganography: seeing the unseen,” IEEE Computer, February 1998, pg 26.
- B. Herre, Jurgen, and Christian

Neubauer, “Digital watermarking and its influence on audio quality,” 105th Audio Engineering Society Convention, Sept 26 to 29, 1998, San Francisco, CA.

C. Herre, Jurgen, and Christian Neubauer, “Audio watermarking of MPEG-2 AAC bit streams,” 108th Audio Engineering Society Convention, Feb 19 to 22, 2000, Paris.

D. Allamanche, Eric, and Jurgen Herre, “Compatible scrambling of compressed audio,” Proceedings of the 1999 IEEE Workshop on Applications of Signal Processing to Audio and Acoustics, Oct 17 to 20, 1999, New Paltz, NY.

E. Allamanche, Eric, and Jurgen Herre “Secure delivery of compressed audio by compatible bit-stream scrambling,” 108th Audio Engineering Society Convention, Feb 19 to 22, 2000, Paris.

F. Cravotta, Nicholas, “Encryption: more than just complex algorithms,” EDN, March 18, 1999, pg 105.

G. Schneier, Bruce, Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition, ISBN # 0471117099, John Wiley & Sons, 1995.

tions via the Commission's OPIMA (Open Platform Initiative for Multimedia Access).

Ideally, the content should be decoupled from its access rights, so that if a consumer upgrades or replaces equipment, to which the access rights frequently link, he or she need not obsolete an existing media-library collection. If the security system benefits only the content creators and distributors, consumers' lukewarm response shouldn't be surprising. If, however, security safeguards pacify content developers' concerns and therefore enable consumers to access a broader and richer set of media than they've been able to enjoy in the past, the consumers' acceptance will be more enthusiastic. Examples of richer media include higher resolution images; high-fidelity, multichannel surround sound; smaller files for a given quality level; and otherwise-unavailable clips,

such as concerts, music videos, and interviews.

Ultimately, the content developers are free to put whatever restrictions they choose on their media. They can prohibit decoded audio from passing over a digital connection to speakers or digital-video streams from passing to a monitor. They can restrict the playback rate over these digital channels to prevent high-speed duplication. They can embed "watermarks"—copyright and usage-rights information—that obstruct playback or otherwise restrict usage with noncompliant systems (see sidebar "Back to basics"). They can even attempt to retrofit media to prohibit copying and use creative differentiation between the terms "can duplicate" and "are able to duplicate" to tip-toe around legal issues (see sidebar "Belatedly closing Pandora's box"). But the more restrictions they and, therefore, you place on usage, the more complicat-

ed the systems become, increasing the potential for end users' frustration. And, because compliance with industry consortiums such as the (SDMI) Secure Digital Music Initiative is voluntary, not mandatory, the first major content developer or distributor that loosens its restrictions in response to predicted or actual consumer confusion, lowers the bar for everyone.

ONLY AS STRONG AS ITS WEAKEST LINK

Figure 1 shows one possible digital-media-distribution system of today for technologically savvy users or of the near future for everyone else. The first point of digital-media downloading will probably be a PC using a cable modem or an ADSL connection. However, it could also be a cable, terrestrial or satellite digital set-top box, a media server, an Internet-enabled digital audio or video player, or even an advanced cellular phone or personal digital assistant.

BELATEDLY CLOSING PANDORA'S BOX

As Hollywood and the consumer-electronics companies drag their feet in finalizing the Secure Digital Music Initiative specification, they ironically exacerbate the copyright-infringement problem by continuing to churn out audio CDs without any security whatsoever and DVD videos with already-compromised illegal-access safeguards. Efforts under way by a number of vendors strive to retrofit digital media with encryption and watermarking capabilities, but legal restrictions and potential hardware and software incompatibilities limit their success.

The Copyright Act of 1976 allows consumers to make as many copies of media for their own use as they want and to transfer all of these copies to another person. (Sharing with others, however, is not allowed, except in academic settings.) The act's 1992 amendment (commonly known as the Audio Home Recording Act) somewhat restricted this consumer freedom for digital-audio media,

prohibiting subsequent duplication of first-generation digital copies in conjunction with the Serial Copy Management System (SCMS).

Production of any system that circumvents SCMS is illegal, but so too is any approach that doesn't allow consumers to make first-generation copies of their legally obtained digital music. Some of the copy-restricting products now under development, although perhaps acceptable outside the United States, come close to violating or blatantly violate consumer rights under the Home Audio Recording Act. And this discussion concerns only audio. The Macrovision copy protection embedded within the analog output of DVD video players, as well as encoded in some videocassettes and videodisks, reflects the fact that even analog duplication of video content is illegal. The 1998 Digital Millennium Copyright Act, whose legality the US Supreme Court has yet to determine, goes one step further in outlawing attempts to circum-

vent any copyright-protection scheme.

Both Ç-Dilla Labs with AudioLok and Midbar Tech with Cactus Data Shield have developed copy-protection schemes that, by inserting small amounts of error data, block playback and, therefore, "ripping" of audio CDs on computer CD-ROM drives. According to the manufacturers, dedicated audio-CD players, because of their greater tolerance of media errors, can still play altered audio CDs (**Reference A**). However, consumer feedback suggests that reality falls short of this goal. Both systems can optionally disable a CD player's digital output, an infringement of consumer rights under the Home Audio Recording Act and of the Red Book CD standard. Undeterred, TTR Technologies, whose MusicGuard technology also blocks duplication of audio content on CDs, is working on extending its technology to DVDs.

Divx may be dead, but companies are still trying to figure

out how to render CDs and DVDs unplayable after a certain time span or number of viewings. Spectra Science, one of the leading restricted-playback proponents, claims to have figured out how to ensure that, once a consumer opens any optical media's packaging, the disk will play only for a content-distributor-specified period of time. A touted environmentally friendly chemical that the company applies to the disk is the secret, and the last step in the production process sets the decay duration. Unlike Divx, Spectra Science's approach requires neither an expensive, custom DVD player, nor that the player connect via phone line to a server for authentication and, some feared, Big Brother snooping of consumer viewing habits.

REFERENCES

A. Starrett, Robert A, "Recording at the speed of sound," *eMedia*, May 2000, pg 28.

Once consumers access a copy of the content, they might want to stream, copy, or move it to other media peripherals in their home or office. A variety of distribution mechanisms is possible, including Ethernet cable, IEEE 1394, and USB 2.0, home-phone-line networking, power-line-network connections, or even wireless. And, to play the file, why bother with the multiple analog-to-digital and digital-to-analog conversions, resolution limitations, and noise coupling, all of which degrade quality, of traditional audio and video cable? Instead, your customers will probably want to run a pure-digital connection to their speakers over S/PDIF (Sony/Philips Digital Interface) or USB and to a display over a DVI (Digital Visual Interface). At no point in this process, however, can unprotected digital data be "in the clear" (also called "plaintext") so that people can copy it.

Regarding downloading versus streaming, the content distributors would probably prefer to transmit only a temporary, quickly discarded bit stream to each customer. Imagine, for example,

paying a monthly subscription fee to a record label and, in exchange, being able to access any song from any album in that label's catalog 24 hours a day, seven days a week. This scenario maintains maximum distributor control over the content, but it doesn't let a user listen to the music on a non-Internet-tethered device. Consumers are also familiar and comfortable with going to record stores and purchasing tapes and CDs; the e-commerce analogy is a digital music file. So, a DMX (Digital Music Express)-like distribution system for music will probably supplement but not replace downloading and archiving, though streaming within the home, such as from a PC to an audio receiver via a Turtle Beach AudioTron or an equivalent, is feasible.

Streaming-only delivery of video material is a more likely scenario, replicating today's pay-per-view and cable-channel subscriptions and partially driven by the huge sizes of video files even after MPEG-2 and other lossy-compression schemes. However, some consumers will undoubtedly be willing to pay an addi-

tional fee for archiving capability. In general, you should anticipate some resistance if you provide no ability to record digital broadcasts, given that analog-broadcast archiving is possible. And, just as individuals rent or even buy DVDs and video tapes so that they can start, pause, and finish viewing the content at their leisure, there'll most likely be a demand for similar capabilities in the digital age. Digital-video-capture capability at degraded quality levels is one possible compromise.

In differentiating between streaming and downloading-and-playing usage models, it's also important to distinguish between the ability to view material and the ability to capture or copy it. This distinction is key to resolving the misconception regarding the infamous DeCSS (content-scrambling system) utility, which circumvented the encryption for DVDs. Duplication of DVD media has *always* been technically possible, though the high cost of writable DVDs and drives currently makes it economically unfeasible. DeCSS simply lets you *view*

SECURING—AND CIRCUMVENTING—AT HIGH SPEED

A key part of the reason that your chosen encryption system should be upgradable, aside from the potential for cracking due to inadvertent disclosure of keys, is the ever-increasing performance of stand-alone and multiple networked computers. Moore's Law dictates that today's computer hardware, using brute-force techniques, takes much longer than next-generation hardware will to calculate a key of given bit length. This acceleration is especially true when dedicated logic gates rather than a general-purpose CPU executing software runs the key-exposing algorithms.

For example, at this February's ACM/SIGDA International Symposium on Field Programmable Gate Arrays (FPGA 2000), representatives from the University of California—Los Angeles disclosed the results of work they'd done with several-year-old FPGA technology, specifically Xilinx 4085XLA devices

(**Reference A**). In a four-FPGA design running at 16 MHz, they ran sieve-factoring operations 28 times faster than similar calculations in software on an UltraSPARC workstation. By moving from 70- to 8-nsec SRAMs, they estimate, they can boost the FPGA design to 100-MHz operation and achieve a 160-times speed increase over the UltraSPARC alternative. With this level of performance, the presenters estimated, they would require only two months to break RSA (Rivest, Shamir, and Adelman)-129.

To combat fast hardware-based cracking, you might want to embrace your enemy and consider using FPGAs. They combine the in-system upgradability of software-based approaches with the high performance of a hard-wired ASIC, and the logic block structures are ideal for implementing the types of arithmetic functions common in encryption and decryption. At

FPGA 2000, representatives from the Worcester Polytechnic Institute (Worcester, MA) used Xilinx XCV1000s to implement the Serpent block cipher (one of the Advanced Encryption Standard candidates) at encryption rates beyond 4 Gbps (**Reference B**). The researchers evaluated four design approaches with varying gate counts and speeds.

The 2.44- to 37.97-MHz, FPGA-resident alternatives were 30 to 952 times more efficient in number of clock cycles than a software-based implementation of the same algorithm running on a 200-MHz Pentium Pro workstation. The FPGA approach also outperformed the software implementation by two to 180 times. Xilinx reported the results of a similar study at April's IEEE Symposium on Field-programmable Custom Computing Machines (FCCM 2000) (**Reference C**). Using the company's XCV150 FPGAs with Java-

based dynamic partial-reconfiguration techniques, Xilinx engineers achieved 10.7-Gbps encryption performance using the DES (Data Encryption Standard) algorithm.

REFERENCES

A. Kim, Hea Joung, and William H Mangione-Smith, "Factoring large numbers with programmable hardware," ACM/SIGDA International Symposium on Field Programmable Gate Arrays, Feb 10 to 11, 2000, Monterey, CA.

B. Elbirt, AJ and C Paar, "An FPGA implementation and performance evaluation of the Serpent block cipher," ACM/SIGDA International Symposium on Field Programmable Gate Arrays, Feb 10 to 11, 2000, Monterey, CA.

C. Patterson, Cameron, "High performance DES encryption in Virtex FPGAs using JBits," IEEE Symposium on Field-Programmable Custom Computing Machines, April 17 to 19, 2000, Napa, CA.

DVD content as well as defeat region coding. It's also important to note that the developers of DeCSS didn't break the CSS algorithm itself. In attempting to create a Linux-based DVD player program, they stumbled across an unprotected access key in the Xing Technology DVD player they were reverse-engineering and, from that 40-bit key, deduced more than 100 other valid keys.

"Cracking an algorithm is far less common than cracking an implementation of that algorithm," says Mark Ashida, president and CEO of media-security-software company and Intel spin-off PassEdge.

Streaming media, in light of its impermanent nature, can tolerate a less robust encryption scheme than downloading-and-playing media, which is fortunate because the near-immediate-response expectations of streaming viewers don't allow for complex encryption and decryption calculations. However, the encryption must be distributed throughout the media, not just in the file header, so that illegal tapping into the bit stream partway through the broadcast is impossible. Typically, you want to reauthorize the connection using a new key pattern every fraction of a second to few seconds. Any evaluation of encryption-algorithm alternatives must also consider that the low cost expectations of consumer-electronics equipment are at odds with the high processing power, memory, and gate-count requirements of robust security protocols.

Given enough time and processing horsepower, a power can use brute force to crack any encrypted data set (see sidebar "Securing—and circumventing—at high speed"). Repeatedly tossing data patterns at an encrypted packet until you stumble across a key that works, though, is not the same thing as finding a hole in the algorithm itself. Your job is to come up with an approach that takes at least as long to circumvent as the time beyond which media's worth becomes negligible. Particularly for downloading-and-playing scenarios, an upgradable algorithm is valuable so that, when someone *does* crack it, you can reinforce it via a longer key set or other techniques. An ideal algorithm also encompasses renewability: the ability to detect and block access by a compromised platform, such as a player attempting to use a key that the content developer has voided.

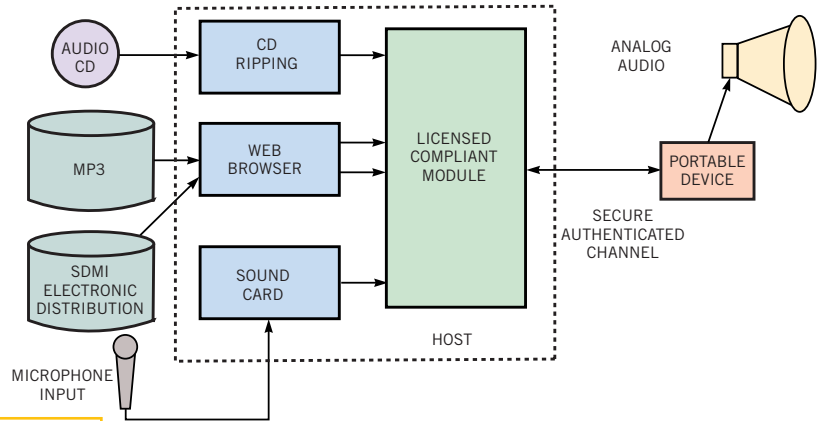


Figure 2

The SDMI protocol contains multiple software levels that both isolate application software from low-level hardware details and ensure secure decryption, decoding, and transcoding of digital media (courtesy Creative Technology).

Lack of renewability is a key limitation of many of today's security systems, such as the smart-card-based techniques that satellite receivers, CSS for DVDs, and the analog-video-based Macrovision system use. Macrovision modifies the video signal to overwhelm the fast-reacting AGC (automatic-gain-control) circuits of VCRs but not the slower reacting AGCs in TVs. An Internet search using the word "Macrovision," however, will uncover a number of "video stabilizers" and software programs that can disable Macrovision or otherwise restore the original video signal. Also, secure delivery of media to customers is only half the task. Content distributors would like to track their customers' usage patterns, both for planning future products and for targeting consumers for advertising on related products. You need to balance these suppliers' desires with your customers' rights to privacy. Not everyone would like others to know what types of books they read, pictures or movies they look at, or music they listen to.

IDENTIFYING THE RECIPIENT

Even if a user can download a file, the media it contains is often an altered version of the original. It's not only encrypted but also watermarked. The platform containing the downloaded file then becomes in effect a security server of its own, distributing further media variants.

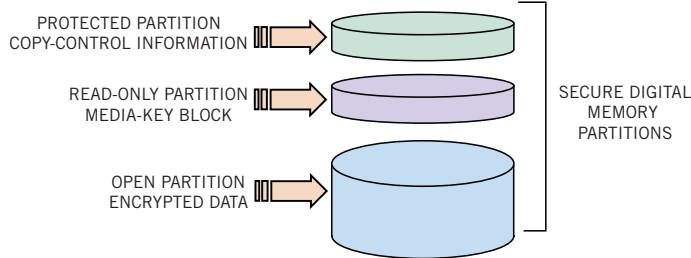
To better understand this concept, consider the SDMI scheme (Figure 2). SDMI requires that any device storing digital audio contain a 32-bit predefined

manufacturer ID or 128-bit random number to generate security keys. Where does this identifier come from? One possible source is a data pattern embedded within a smart card, parallel-port "dongle," or flash-memory card (Reference 2). Because the decryption key is tied to a removable device, not the player itself, a user can move that media among multiple players. (For example, you can take your songs over to your friend's house to listen to them.) However, this approach has downsides, too. If the media is lost or irreparably damaged, the rights to the media disappear. Media portability also raises the specter of illegal duplication, a scenario that can only be detected if, for example, two people attempt to listen to the same music file at the same time using the same key.

The other alternative is to generate security keys from an embedded ID located within the playback system itself. This identifier could be a code inside the microprocessor, such as in Cirrus Logic's Maverick products or Intel's Pentium III CPU. You might also tie the security keys to the volume ID of a hard drive or to the MAC (media-access-control) address of a network card, or to a dedicated security chip as IBM has done with its 300PL PC. The downside here, aside from the lack of media portability, is that should the user replace the ID-sourced component in the future, the previously generated keys will become invalid. Regardless of the key generation "seed" source, the process of generating keys must be as random as possible. For example, the firmware hub of Intel's i810, i815, i820,

and i840 core logic chip sets creates random numbers through

Figure 3



Secure Digital cards store not only encrypted digital media files, but also a card-specific identifier and a table of IDs for trusted playback devices (courtesy Sandisk).

sensing and amplifying thermal noise patterns across undriven resistors, and a secure communication channel links the firmware hub to the I/O hub.

From an encryption standpoint, SDMI doesn't care which of a multitude of possible encryption and decryption and compression algorithms you choose. As Matt Perry, vice president and general manager of the Embedded Processor Division at Cirrus Logic, describes it, the encryption portion of the SMDI protocol is only a functional specification and, therefore, is open to numerous encryption and audio-codec implementations. However, DMI's Version 1.0 specification defines a specific watermark technique that Verance developed and DVD Audio also plans to incorporate. It lets you make, by default, four copies—adjustable from zero to an infinite number of copies—of the downloaded media for distribution to and movement among devices such as other PCs or portable audio players. You must check a copy back in before you can make another. SDMI also specifies multiple access levels. SDMI 1.0-compliant devices must search for the Verance watermark at least every 15 seconds. SDMI-compliant hardware will carry the DMAT (Digital Music Access Technology) stamp of approval.

The not-yet-finalized SDMI 2.0 specification defines another set of watermarks. They include a "do-not-import-if-previously-compressed" flag that would prevent playback of, for example, MP3 files that users obtained by some means other than from their private audio-CD collections using an SDMI-compliant "ripping" (extracting-to-hard-drive) program (Reference 3). SDMI 1.0-compliant players must search for the 2.0-indicating "trigger" and then cannot play SDMI-compliant media until the user upgrades the player firmware. These additional proposed watermarks may inhibit users' abilities to play their MP3 libraries. If implemented in the final specification, these additional security

measures will likely trigger a consumer uproar like the one that the "millennium trigger" caused during the early drafts of the SDMI 1.0 specification.

SDMI 2.0-compliant firmware isn't the only means by which the consortium members hope to control consumers' usage patterns. If the media that stores the files can interrogate the player and block playback if it detects the presence of a compromised unit, additional access rights become available. This concept is central to the definition of the SD (Secure Digital) card, defined by the so-called 3C (three-company) Entity: Matsushita, Sandisk, and Toshiba. SD cards contain a protected media-key block describing all valid players (Figure 3). Each time a player containing an SD card connects directly or indirectly to the Internet, the connection causes an update of the media-key block contents, if necessary, to reflect players whose keys have been revoked. Vendors should also keep media-key-block information up to date in the SD-card manufacturing line.

SD cards incorporate the CPRM (Content Protection for Recordable Media) Protocol, which, along with the CPPM (Content Production for Prerecorded Media) Protocol, the 4C (four-company) Entity—IBM, Intel, Matsushita, and Toshiba—developed. CPRM and CPPM derive from the same CSS encryption scheme that the 4C Entity developed for DVD video and DVD audio disks. DVD Video's circumvented security, which DeCSS exemplifies, has compelled DVD-audio advocates to delay mass production until they can come up with a more robust alternative encryption approach. However, the revocation

capability of CPRM has enabled SD deployment to proceed.

Current encryption technologies as well as those now under development promise to enable high-speed and easy interchange of digital media within homes and offices. Standards bodies have yet to endorse an official approach for IEEE 1394, but the emerging de facto standard appears to be the Digital Transmission Copy Protection algo-

rithm that the 5C (five-company) Entity—Hitachi, Intel, Matsushita, Sony, and Toshiba—developed. Encryption over TCP/IP (Transmission Control Protocol/Internet Protocol) has existed in numerous forms for some time and applies to traditional Ethernet as well as to HomePNA (Home Phone Networking Alliance) and HomePlug Powerline Appliance network connections. Encryption, authentication, and frequency-hopping are integral to the Bluetooth, HomeRF, and IEEE 802.11 specifications. Both powerline and wireless networking techniques must comprehend sufficient safeguards to ensure that your neighbors can't illegally access the media. You can also apply the DTCP (Digital Transmission Content Protection) Protocol for IEEE 1394 to USB.

SHUFFLING THE BITS

What if your customer wants to connect a set of digital-interface speakers to his or her audio playback device or hook up a video-playback unit to a digital flat-panel display or CRT? These links also must be secure. Most of today's digital speakers employ S/PDIF connections, whose limited SCMS (Serial Copy Management System) encryption hasn't stood up to the test of time. Until encryption support becomes pervasive in USB-equipped devices, content developers will have muted enthusiasm for the concept of audio-playback systems with "live" digital outputs.

IEEE 1394 currently provides insufficient bandwidth to enable the transmission of uncompressed high-resolution video streams. For this purpose, you must turn to the DVI protocol, which Silicon

Image developed under the name Panellink technology and which is also called TMDS (transition-minimized differential signaling). DVI's secure variant, which Intel announced and Silicon Image demonstrated in February at its Developer Forum, is HDCP (High-bandwidth Digital Copy Protection) (Figure 4). Silicon Image is currently shipping samples of first-generation HDCP-aware DVI Sil 168 transmitter and Sil 861 receiver chips and slates production of both for the third quarter of 2000.

Like SDMI for audio, HDCP supports the concepts of *authentication* to verify that a display device is licensed to receive protected content, *encryption* of the transmitted video to prevent "eavesdropping" on the protected content, and *renewability* to enable the revocation of compromised devices. HDCP's hybrid-block/stream-cipher approach encrypts data at the transmission end of each 1.65-Gbps channel and decrypts it at the other side. The approach uses the more robust block cipher during authentication. Both the authorized host and display device have access to a set of secret keys that the HDCP license administrator supplies. The secret keys consist of an array of 40 56-bit secret device keys and a corresponding 40-bit binary key-selection vector (KSV). The host initiates authentication by sending an initiation message containing its KSV and a 64-bit value. The display device responds by sending a response message containing its KSV. The host confirms that the received KSV has not been revoked.

At this point, the two devices can calculate a shared value, which, if both devices have a valid set of keys, is equal. The devices use this shared value in the encryption and decryption of the protected content. Authentication has now been established, and reauthentication occurs every 2 sec, or each time the connection is lost for any reason. A faster, bitwise-exclusive-OR-based stream cipher handles content delivery. If the HDCP license administrator discovers that the security of

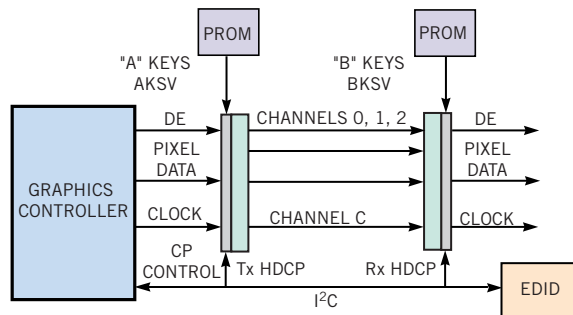


Figure 4

High-speed stream encryption of the display information, plus periodic block encryption for authentication, come together to form the HDCP scheme for digital displays (courtesy Silicon Image).

a certain display device has been compromised and the secret device keys are exposed, the administrator places the KSV that matches the compromised device key on a revocation list. System-renewability messages (SRMs), which the host manages, contain this list. The host must update its revocation list when it receives a valid, newer SRM than that currently held in memory. SRMs can be presented to the host in prerecorded or broadcast content, or received from another compliant device with a newer SRM. Encryption and decryption logic add approximately 10,000 logic gates to the transmitter- and receiver-chip designs.

UNDER THE HOOD

So much for media that passes between systems. What about security within a system? The degree of vulnerability caused by an "in-the-clear" digital bit stream passing between chips inside a system depends on how "open" the system is. A proprietary, nonupgradable set-top box, for example, realistically isn't a point of vulnerability for any but the most hard-core hackers, who would think nothing of tapping into a board trace or probing a packaged IC's leads to siphon off a digital bit stream.

On the opposite end of the spectrum, however, consider PCs. A number of available third-party software packages disable Macrovision protection for DVD movies, enabling dubbing to video recorders through a graphics card's video output. High Criteria's Total Recorder software intercepts a digital-audio bit

stream on the way to the PC's sound card. Streambox VCR performs a similar function for video. And the sound cards in some PCs digitally output any audio bit stream routed to them and ignore SCMS copy-protection bits at their digital inputs.

The emergence of digital-TV receivers and decoder hardware and software for PCs exposes another potential source of duplication. In an approach such as the one that Raviscent Technologies advocates with its CinePlayer DTV, a low-cost add-in card handles the digital-TV reception and demodulation tasks and then sends the

combined audio, data, and video bit stream across the PCI bus to software running on the host CPU for demultiplexing, decoding, and output. A rogue PCI add-in card could easily intercept this (albeit perhaps encrypted) bit stream. Even a more hardware-intensive approach, such as one that TeraLogic advocates, isn't immune to piracy. The company's Janus chip relies on external software to handle audio decoding and passes decoded video data to a graphics card over an easily tapped VIP 2.0-compatible port.

The PC is perhaps the most extreme—but not the only—example of an open architecture. Should the OpenCable initiative turn into real systems, for example, those products will also be, by virtue of their openness, susceptible to hacking. Fortunately, semiconductor-integration trends are helping to solve the problem. Advanced audio-playback chips, such as Cirrus Logic's Maverick line and Micronas' MAS3509E, both decrypt and decode an incoming secure bit stream within the same device, never revealing the system-specific key. The Micronas device even integrates the D/A converter, so that neither the decrypted nor the decoded digital-audio information is ever exposed.

Future operating-system enhancements, placing system-specific encryption at their core instead of as add-ons, will also help boost security while maintaining platform openness. Microsoft spent a lot of time at April's Windows Hardware Engineering Conference (WinHEC) talking about this subject,

FOR MORE INFORMATION...

For more information on products such as those discussed in this article, enter the appropriate numbers at www.ednmag.com/infoaccess.asp. When you contact any of the following manufacturers directly, please let them know you read about their products in *EDN*.

COMPANIES

AT&T's a2bmusic subsidiary

1-212-583-6800
www.a2bmusic.com
Enter No. 319

Baltimore Technologies (and GTE CyberTrust subsidiary)

1-781-455 3333
www.baltimore.com
Enter No. 320

Cirrus Logic

1-512-445-7222
www.cirrus.com
Enter No. 321

Cognicity

1-952-841-7100
www.cognicity.com
Enter No. 322

Destiny Media Technologies

1-604-609-7736
www.destiny-software.com
Enter No. 323

Digimarc

1-503-885-9699
www.digimarc.com
Enter No. 324

Excalibur Technologies

1-703-761-3700
www.excalib.com
Enter No. 325

Fraunhofer Institute for Integrated Circuits

+49 (0) 9131 / 776 0
www.iis.fhg.de
Enter No. 326

IBM

1-914-765-1900
www.ibm.com
Enter No. 327

Intel

1-503-696-8080
www.intel.com
<http://developer.intel.com/ial/security>
<http://developer.intel.com/software/security>
Enter No. 328

InterTrust Technologies

1-408-855-0100
www.intertrust.com
Enter No. 329

Liquid Audio

1-650-549-2000
www.liquidaudio.com
Enter No. 330

Macrovision and Ç-Dilla Labs subsidiary

1-408-743-8600
www.macrovision.com
www.c-dilla.com
Enter No. 331

Micronas Semiconductors

1-408-526-2080
www.micronas.com
Enter No. 332

Microsoft

1-425-882-8080
www.microsoft.com
Enter No. 333

Midbar Tech

972-3-5186666
www.midbartech.com
Enter No. 334

PassEdge

1-503-466-8400
www.passedge.com
Enter No. 335

RPK SecureMedia USA

1-415-563-1800
www.rpk.com
Enter No. 336

Silicon Image

1-408-616-4000
www.siimage.com
Enter No. 337

Sony

1-201-930-1000
www.sony.com
Enter No. 338

Spectra Science

1-401-274-4700
www.spectra-science.com
Enter No. 339

TTR Technologies

972-9-7662394
www.ttrtech.com
Enter No. 340

Verance

1-858-677-6522
www.verance.com
Enter No. 341

ViaTech

1-508-647-0464
www.elicense.com
Enter No. 342

Wave Systems

1-413-243-1600
www.wave.com
Enter No. 343

Xilinx

1-408-559-7778
www.xilinx.com
Enter No. 344

STANDARDS BODIES AND CONSORTIA

1394 Trade Association

1-408-748-9416
www.1394ta.org
Enter No. 345

4C Entity

www.4centity.com
Enter No. 346

Bluetooth Special Interest Group

www.bluetooth.com
Enter No. 347

Digital Display Working Group (DVI)

www.ddwg.org
Enter No. 348

Digital Transmission Copy Protection Licensing Administrator (5C Entity)

www.dtcp.com
Enter No. 349

Electronic Frontier Foundation

1-415-436-9333
www.eff.com
Enter No. 350

Home Phonenumbering Alliance

www.homepna.org
Enter No. 351

HomePlug Powerline Alliance

www.homeplug.org
Enter No. 352

Home Recording Rights Coalition

1-800-282-8273
www.iec.ch/opima
Enter No. 353

HomeRF Working Group

1-503-291-2563
www.homerf.org
Enter No. 354

International Electrotechnical Commission

+41 22 919 02 50
www.iec.ch/opima
Enter No. 355

Motion Picture Association

1-818-995-6600
www.mpa.org
Enter No. 356

Music Publishers Association

1-212-327-4044
www.mpa.org
Enter No. 357

Recording Industry Association of America

1-202-775-0101
www.riaa.org
Enter No. 358

Secure Digital Association

1-831-623-2107
www.sdcard.org
Enter No. 359

Secure Digital Music Initiative

1-858-826-2655
www.sdmi.org
Enter No. 360

USB Implementers Forum

1-503-296-9892
www.usb.org
Enter No. 361

OTHER COMPANIES MENTIONED IN THIS ARTICLE

Adobe Systems

www.adobe.com

AMD

www.amd.com

America Online

www.aol.com

Creative Technology

www.creative.com

DMX

www.dmxmusic.com

Gnutella

gnutella.wego.com

High Criteria

www.highcriteria.com

Hitachi

www.hitachi.com

Matsushita

www.matsushita.co.jp

Napster

www.napster.com

Nullsoft

www.nullsoft.com

Ravisent Technologies

www.ravisent.com

RealNetworks

www.realnetworks.com

Sandisk

www.sandisk.com

Scour.net

www.scour.com

Streambox.com

www.streambox.com

TeraLogic

www.teralogic-inc.com

Toshiba

www.toshiba.com

Voyetra Turtle Beach

www.voyetra-turtle-beach.com

Xing Technology

www.xingtech.com

SUPER CIRCLE NUMBER

For more information on the products available from all of the vendors listed in this box, enter No. 362 at www.ednmag.com/infoaccess.asp.

which is a key feature of the company's follow-on to Windows 2000, code-named Whistler, and its successor to Windows 98, code-named Millennium Edition. These enhancements are by no means straightforward to implement. They require changes not only to the operating system but also to the BIOS, and they must incorporate a means of uniquely identifying the system. A unique ID embedded in the processor, which is the least likely hardware subsystem to get replaced, is the most obvious means of achieving this goal.

Intel received much backlash after its public disclosure of the Pentium III processor's serial number, however, and the company subsequently developed a utility that disables the serial number and announced removal of the serial number in the follow-on Williamette CPU. Competitor AMD was therefore reluctant to follow in Intel's stumbling footsteps. In a similar vein, Microsoft pointed out at WinHEC that any user concerned with privacy can disable any identification scheme the company comes up with,

even though such a step might prohibit access to certain content. Third-party hardware and software developers will also need to add security hooks to their drivers so that they won't lose access if a certain media type insists on operating only with secure programs. □

REFERENCES

1. Dipert, Brian, "Now hear this," *EDN*, Feb 3, 2000, pg 50.
2. Dipert, Brian, "Memory cards: designing with a full deck," *EDN*, May 25, 2000, pg 69.
3. Starrett, Robert A, "Ripping off recordings; extraction do's, don'ts and do'ers," *eMedia*, July 1999, pg 34.
4. DeCarmo, Linden, "Pirates of the airwaves; new technologies for audio copy protection," *eMedia*, September 1999, pg 50.
5. DeCarmo, Linden, "Safety in numbers; a look at the Secure Digital Music Initiative," *eMedia*, November, 1999, pg 48.
6. Lawton, George, "Intellectual property protection opens path for e-com-

merce," *IEEE Computer*, February 2000, pg 14.

7. Bell, Alan E, "The dynamic digital disk," *IEEE Spectrum*, October 1999, pg 28.

8. Caloyannides, Michael A, "Encryption wars: early battles," *IEEE Spectrum*, April, 2000, pg 37.

9. Drummond, Mike, "The Madison project," *Stereo Review's Sound & Vision*, November 1999, pg 119.

10. Takiff, Jonathan, "Judgement day," *Stereo Review's Sound & Vision*, May 2000, pg 90.

ACKNOWLEDGMENTS

In researching this article, I appreciated the information and insights I received from Wes Brewer and Farshid Sabet of Sandisk regarding SDMI and the SD card, from numerous employees of the Fraunhofer Institute via their Audio Engineering Society conference papers and other documentation, and from Dave Rossum, chief scientist at Creative Technology, via his excellent presentation at this year's WinHEC.