Sean Burak

Protecting the Copyright of Digital Audio and Video Content

Abstract

The combination of faster internet connections and cheaper digital storage opportunities poses a great challenge to copyright holders of digital media. This paper examines three techniques for protecting digital data from unauthorized copying, with focus on the goal, the execution, and the effectiveness of the scheme. Serial Copy Management Systems (SCMS) have already seen widespread use in consumer audio. Encryption has of course been in use for a long time, and has recently been in the spotlight with its application to DVD video data in the form of the Content Scrambling System (CSS). Finally, digital watermarking, the newest of the three technologies, is in the beginning stages of implementation as part of the Secure Digital Music Initiative (SDMI). The paper concludes that, while all three schemes do what they are supposed to, they can all be compromised without much difficulty, some even by casual consumers.

Serial Copy Management System (SCMS)

Serial copy management has been incorporated in consumer digital recorders since the Audio Home Recording Act of 1992 was passed, prohibiting the sale or import of non SCMS compliant devices. The recording industry knows that (much to the delight of music pirates) it is easy to make a perfect digital copy of a piece of music. The basic goal of SCMS is to limit the number of generations of digital copies a consumer can make. The scheme allows unlimited first generation digital copies from the source, but disallows additional digital copies of those first generation copies.

The implementation of SCMS involves both the devices transporting the data and the data itself. The basic idea is to set a digital flag within the data, to signal to the recorder whether or not copying is permitted. The SCMS flags are two bits long, and are interpreted as follows: `00` means that unlimited copying is allowed. `10` means that no copying is allowed. `11` means that one copy is permitted. The recorder receives these bits at the beginning of the stream of audio data. If the bits are read as `10`, then no copy is made. If read as `11`, a copy is made, but the bits are set to `10` in the resulting copy. If `00` is read, a copy is made with no change to the flag bits.

While this scheme is technically effective, it can be easily compromised by inserting a device between the player and recorder, which is capable of reading and changing these bits. Such a device is called an SCMS stripper. Additionally, bugs in the software in consumer devices can often allow the average consumer to override the protection without any additional hardware. Finally, it should be noted that this scheme is looked down upon by many consumers, as it poses limitations on people working legally with their own digital media, yet does not stop true pirates from distributing their illegal material (as long as they copy it from the original, it is allowed by the technology).

Sean Burak

Content Scrambling System (CSS)

The Content Scrambling System is a type of encryption used to prevent unauthorized access to the data on a DVD. The general principle is to encrypt the data on the disk such that it can be decrypted and accessed only by hardware and software that is authorized to do so. This encryption is intended to prevent people from illegally copying or distributing the video data.

Again, the success of this system depends on both the data involved and the hardware (such as DVD players) and software (such as DVD playing programs for computers) used to access the data. The basic implementation of this scheme is as follows:

1. About 400 valid player keys exist. Each DVD player has one (or sometimes a few more) valid player key.
2. Each disc is encrypted such that a disc key is required to unscramble the information. 400 encrypted versions of this disc key are stored on the disc, each one encrypted with one of the 400 valid player keys.
3. A hash code of the decrypted disc key is stored on the disc. This is used for the player to verify that it has found the correct disc key, while not allowing the disc key to be read directly.
4. Disc keys and player keys are 40 bytes long (this is the maximum encryption key length allowed under United States export laws.

This is what happens, typically, when a DVD is played in an approved player:

1. The player attempts to decrypt each of the 400 encrypted disc keys using its player key.
2. If the encryption is successful, the hash code of the decrypted disc key will match the hash code stored on the disc. The player proceeds, using the decrypted disc key to unscramble the encrypted disc contents.
3. If none of the 400 keys are correct, the player retries with its other player keys, if it has any.

All of this is transparent to the end user, happening quickly in the background while the disc is booting. Clearly, a piece of software or hardware will not be able to access the data without a valid player key.

This scheme, while seemingly effective, is considered by many to be laughably weak. For starters, it is clear that with enough time, one could run through all 2^{40} possible disc keys until finding the correct one. Even worse, one could run through all 2^{40} possible player keys until one of the 400 valid ones is found which can be used to decrypt every DVD. In fact, this has been done, and has been proven to actually be possible in only 2^{25} moves! Worse, this scheme relies on each player keeping its own key(s) secret. The weakness of this approach became apparent when CSS was originally compromised due to one player manufacturer (Xing Technologies) leaving their key unencrypted in their software. The CSS technology was originally developed to overcome this type of compromise by providing the option to remove any compromised player key from the valid list of player keys in all future software. Unfortunately, knowing one (or more) valid player keys makes finding all the others much easier, and in no time at all every player key was found by crackers. While more difficult to crack than SCMS, CSS is an equally ineffective means of data protection.

Secure Digital Music Initiative (SDMI)

SDMI is the latest attempt by the recording industry to incorporate a copyright protection scheme into newly released music. The recent boom in trading of mp3s containing copyrighted content has been a very strong motivation for the development of SDMI. The general principle of SDMI is to stamp each officially released copyrighted piece of music with an identification that cannot be removed. If the work is ever copied and distributed without authorization, a means of tracking down the illegal distributor is possible.

SDMI relies on a technique called digital watermarking. Similar schemes have already been successfully used to insert identification data into digital images. To be effective, a digital watermark should have at least the following properties:

1. The extra data must not interfere with the important audio (or other) data. It must be transparent to the end consumer.
2. The watermark must remain intact through copying, encoding, decoding, and any other process that alters the data in a way that leaves the audio intact.
3. The watermark must not be able to be removed, even if one knows how to detect and interpret it.

The watermark may additionally carry copying information (similar to SCMS) that an SDMI compatible device can interpret. Unlike SCMS though, the watermark can not be stripped from the data. Many companies have proprietary methods of creating watermarks that contain the above properties to varying degrees.

The effectiveness of digital watermarking seems to be much greater than the previously mentioned technologies. Watermarks can be used to track distribution, detect data tampering, and more. Recently, a hacking competition was held in order to test the four current watermarking techniques under consideration for SDMI. Participants have reported that all four watermarks were successfully removed, although the SDMI committee has remained suspiciously quiet regarding the issue. It will be interesting to watch the development of the SDMI technology. SDMI supporters are adamant that before long, all digital audio devices will be SDMI compliant, and all copyrighted music will contain SDMI security protection. Many consumers argue that digital watermarks will never be in mainstream use, as they can never be 100% undetectable by the ear. Expect to hear a lot more from both sides in the near future.

Conclusion

While it is not possible to create a perfectly secure data protection scheme, it is clear that some (SCMS, CSS) fail miserably, while others (SDMI) may fare better when presented to the real world. With each attempt at creating a secure digital distribution scheme comes a barrage of attempts to crack the scheme. If a strong enough method of protection can be developed (and if the record and film industries can create enough value in their products for their customers), the mainstream copying and distribution of copyrighted data will slow down. Unfortunately for the entertainment industry, no such technology has yet been developed.

Protecting the Copyright of Digital Audio and Video Content (Slides)

Sean Burak

SCMS – Serial Copy Management System

CSS – Content Scrambling System

SDMI Secure Digital Music Initiative

Sean Burak

SCMS – Serial Copy Management System

- Designed to control the copying of digital music
- 1992 Audio Home Recording Act
- Unlimited single generation digital copies allowed
- No copying of the first generation copies
- Implemented with copyright bit pairs:

  00 – Unlimited copying allowed

  10 – No copies allowed

  11 – One copy allowed

Sean Burak

SCMS – Serial Copy Management System

- Technically effective
- Easily defeated
- SCMS Stripper devices
- Buggy consumer recorders
- Not sufficient
- No limitation on first generation copies
- Too limiting for legitimate users

Sean Burak

CSS – Content Scrambling System

- Encryption of DVD data
- Only approved CSS compatible players and software can decrypt the data
- Prevent unauthorized copying of decrypted data
- Provide control over who can manufacture DVD players

CSS – Content Scrambling System

- Every player has one of 400 valid Player Keys
- Every Disc is encrypted using a Disc Key
- 400 Encrypted versions of the Disc Key are stored on the disc, along with a hash key of the decrypted Disc Key
- Players apply their Player Key to each encrypted Disc Key until one generates the correct Disc Key
- Players use the Disc Key to decrypt the DVDs contents
- Disc Keys and Player Keys are 40 bits long

CSS – Content Scrambling System

- Easily compromised – 2^{40} possible keys, but can be discovered in 2^{25}
- Scheme relies on Player Keys remaining secret
- Xing Technologies left theirs unencrypted!
- Scheme has some leeway for compromised keys
- All Player Keys soon compromised
- A race to write the fastest, smallest deCSS code

Sean Burak

SDMI – Secure Digital Music Initiative

- Formed by record companies for digital audio security
- Motivated by recent mp3 boom
- Based on stamping an identification code on each song that is distributed through the record companies
- ID cannot be removed
- Illegal distribution can be traced to original owner

SDMI – Secure Digital Music Initiative

- Achieved through digital watermarking
- ID data is encoded directly inside the audio stream
- Watermark must:
    - Be completely inaudible (transparent)
    - Remain intact through multiple encoding, decoding, processing and copying stages
    - Not be easily removable from the audio data, even if the means to detect and decode it is widely known
- Watermark may carry copying information (like SCMS) but it cannot be removed

SDMI – Secure Digital Music Initiative

- Very flexible with many applications beyond copyright protection
    - Distribution control
    - Distribution tracking
    - Data tampering detection
- “Hack SDMI” competition
    - Participants claimed SDMI was hacked
    - SDMI committee remains quiet . . .
- Could be a feasible, useful tool

Conclusions

- There is no perfect cure
- For every system developed, there will be countless people ready to attack it
- At some point, every song we hear and video we see must be decoded for it to be understood by us
- Current methods are ineffectual, and future methods are sure to be looked down upon by most consumers
- Entertainment industry must come up with a decent scheme, and must provide value to its customers to deter copiers