System and Method of Fighting Digital Copyright Infringement

Prepared for the USSS, New York Electronic Crimes Task Force,
Recording Industry Association of America, and Universal Music
April 16, 2002
By: Daniel Von Kohorn

The argument is familiar: the protection of intellectual property rights is critical to the viability of intellectual work, including the writing and production of music and movies. This document is prepared in the interest of fighting the illegal distribution of copyrighted media, protecting the value of digitally transferable media, and restoring the economic incentives for artists.

The problem of illegal file sharing is complicated: peer-to-peer (P2P) networks have enabled individuals to download copies of music files from aggregated file servers without compensation to the owner of the copyright.

The solutions to this point have been ineffective. The mean number of simultaneous users on major file-sharing networks is in excess of half a million. Relying on a combination of strategies including legislation, copy protection software, digital rights management, and litigation may provide some relief to the growing problem, however, there may be a far more effective and, at the same time, far less expensive technical solution.

Presented below is an outline of the system and method of file-specific systematic attack on file-sharing networks, with the ultimate goal of eliminating specific media files from public file-sharing systems.

SYSTEM AND METHOD OUTLINE:

1. Install any number of personal computers ("RIAA-PCs") distributed throughout the world, possibly in the homes of RIAA employees or allies.
   - The IP Addresses of the RIAA-PCs should not follow a pattern (i.e. all residing within one IP block)
2. Subscribe each RIAA-PC to a high-speed Internet connection, and install as many concurrent file-sharing systems as possible on each.
   - Wherever possible use common download and upload directories for the various file-sharing systems.
3. Search for, and download, copies of any files you wish to protect ("Protected Files").
   - Specify keywords and other search criteria for each Protected File in order to identify the appropriate files to download. These downloaded files will provide consistency with the meta-data of each pirated files and also cover the breadth of variety in pirated file names and content. Many different versions of each file may exist under different names, quality levels, file formats, etc. However, if searches are specified in a similar manner as other users specify them, then results are likely to include the majority of the pirated files targeted.

4. Upon successful download, overlay additional waveform on MP3 file.
   - This waveform should noticeably disrupt the music periodically and make the pirated file unsatisfactory as a proxy for the original. For example, fluctuate the volume from 100% to 10% periodically, add tones, add silence, etc.
   - The overlay process can be automated: any file added to a designated download directory is then modified with a consistent (or randomized) overlay to the waveform or image.
   - Any incorrect files accidentally included in the search results will be downloaded, manipulated, and shared in unusable form from RIAA-PCs, but so be it--it is an anonymous file-sharing system and people share all kinds of files.
5. Distribute the manipulated file ("Bait File") among the RIAA-PCs, and share each on the most popular file-sharing services.
   - Redundant hosting of Bait Files on each file-sharing network (and across different file-sharing networks) can be facilitated by internally distributing the Bait Files among the RIAA-PCs.
6. Bait Files will dominate the search results when users attempt to download Protected Files.
   - Redundant hosting of Bait Files on large numbers of RIAA-PCs will create consistency in the search results, multiple hosts for higher download prioritization, and greater likelihood of download.
   - Users may still be able to find the original pirated files, but the Bait Files will be very similar and not easily distinguishable as manipulated. Users will instead be forced to download large numbers of the same file and manually test each for quality—a level of complication that will discourage users from seeking and sharing protected files.

Initially, there will be a very large volume of files to download and serve as Bait Files. Other users of file-sharing systems presently find that the downloading and copying of files is quite easy, and RIAA-PC administrators are likely to find the same.

Over time, users will find that their attempts to download protected works will increasingly result in the download of Bait Files. As this occurs, the frustration of both the hosting and downloading of protected files will become prohibitive. Most users download music from file-sharing systems because the identification of files is easy and the quality of the music is good. The strategy proposed above results in the most common keywords becoming useless, and the download quality unusable. As a result, users will become frustrated with online music from the file-sharing systems covered by this strategy, and they will migrate to legitimate music sources.

Likely reactions to this strategy on the part of the file-sharing community will be:

1. Closed networks. These are smaller and have less impact on sales. They also grow more slowly and can be attacked more easily through litigation because they have an organizational structure.

2. Quality screening tools. There will be a constant evolution of the overlay methodology on the part of the RIAA-PCs, and the quality checking software that users may begin to create as a reaction to Bait Files. The inconvenience will make the sharing of protected works a

far less popular activity. The automation of overlays makes the inconvenience for the RIAA minimal.

3. Fragmentation of file-sharing systems. As RIAA-PCs host a critical mass of files on any system, it becomes less attractive and so users will migrate to new systems. However, one of the major attractions of file-sharing systems is the large number of contributors that provide variety of selection. A larger number of smaller file-sharing systems reduces the convenience of searching for any particular file, and so reduces the convenience of file-sharing systems.

4. File-sharing blacklists. As large numbers of Bait files are noticed coming from IP addresses, these IP Addresses may be noted in public or private “Blacklists”, and eliminated from the peer network of default installations of file-sharing software. It is not common or easy for the user to track the IP address of the peer providing each file. Nor is it likely that users will take the trouble to contribute to a public database of Bait File hosts. It is very easy for RIAA-PCs to change IP addresses often. RIAA-PCs may number in the hundreds (thousands?) and be distributed geographically to increase the complexity of any possible blacklist project.

File-sharing systems take advantage of anonymity and under-regulation. The strategy above uses those same powerful characteristics to eliminate the effectiveness of sharing certain selected files.

I would be happy to answer any questions.

Daniel A. Von Kohorn
Chief Technical Officer
Technology Partners (Holdings) LLC
570 Lexington Ave
New York, NY 10022
Phone: 212-759-3022
Fax: 212-759-9184
E-mail: dan@vonkohorn.com
http://tphllc.com