GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Online Music:
The Game of Cat and Mouse Surrounding Licensing

© SANS Institute 2004, Author retains full rights.

Troy Martin
Submitted for GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b (Option 1)
August 19, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

This paper will focus on the principles involved in licensing MP3's and the future evolution of an Internet aware music industry. It will not focus on answering the question of whether or not people should be allowed to download MP3's for free from the Internet.

After the introduction of the MP3 audio format to the Internet community, it was quickly adopted, allowing it to become the most popular digital audio transmission format online. It was an excellent format for storing and playback of music in the digital age. Unfortunately, this format is most commonly associated with the illegal transfer of music as legislated by international copyright protection laws. The media wrote endlessly about MP3's and Napster, the software and network used to easily transfer files in MP3 format. The relative ease of transfer and abundance of MP3's on the Internet sparked alarming concerns within the music industry. The Recording Industry Association of America (RIAA) along with various other artists began to criticize all who illegally transferred their copyrighted material. According to the RIAA website, $4.2 billion of worldwide revenue is lost each year due to copyright infringement.[1]

Numerous entrepreneurs promptly released products onto the market that played MP3's natively. In order to capitalize on this trend, the industry needed to develop a method to support legal file transfers thereby providing fans with music in MP3 or AAC format. The challenge was developing a solution that could generate revenue from the sales of online music.

As long as there is a desire to obtain digital music, the music industry will always remain in a permanent game of cat and mouse. Licensing schemes will continue to be reverse engineered. As fast as new licensing schemes are released, cracks will be nipping at their heels.

What is an MP3?

In order to discuss MP3's, it is important to understand the meaning of "MP3". The MP3 algorithm was published as part of MPEG-1 (Motion Picture Experts Group-1) and the final phase was published in 1995 resulting in the international standard ISO/IEC 13818-3. MP3 (also know as MPEG-1/2 Audio Layer 3) uses an algorithm to code music for later playback on a PC, Hi-Fi Sound System or personal music device. The popularity of MP3's stem from their ability to compress audio while maintaining a quality indistinguishable to the ears of the listener, from that of the original.

CD quality audio is commonly referred to as digital audio sampled at 44.1kHz using 2 x 16bit sampling. Performing a quick calculation, one can determine that

[1] Recording Industry Association of America

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

this requires approximately 1.4Mb of storage space for every one second of audio generated.

$$\frac{441000 samples}{\text{sec}ond} * \frac{2*16 bits}{sample} = 1{,}4111{,}200 bits\ per\ \text{sec}ond\ or \approx 1.4 Mbps$$

A three minute song stored in "CD quality" would therefore require approximately 25.4Mb of storage space. Some proponents of MP3's reason that one can achieve 11:1 compression[2] using the MP3 algorithm. This would effectively reduce the storage space required for the "CD quality" from 25.4Mb to roughly 2.3Mb with no discernable reduction to the audio quality. The ratio is even higher (18:1) for a compression that few people would be able to distinguish from that of the original.

The algorithm depends on a hybrid transformation rendering a time domain signal into a frequency signal.[3] An important characteristic of the algorithm is that it is lossy. This means to say, that it achieves the 11:1 compression by removing bits from the input in order to reduce the space required. The special technique requires removing the bits in such a manner that the human ear may not be able to detect any missing information. This is accomplished through the extensive study and modeling of the characteristics of the human ear.

Can you determine the difference between "CD quality" and an MP3 version of an audio recording? Try this simple test. Convert you favorite music file from CD into MP3 format using the following bit rates: 96, 112, 128, 160, 192, 224, 280, 312, 344 and 384kbps. Listen to the CD audio first, than start at the highest bit rate and work your way backwards listening to each MP3. Next try listening to them randomly and see if you can determine which bit rate was used and which version is the original CD recording. Were you able to distinguish a difference?

Evolution of Audio Music on the Internet

The MP3 Story

MP3's first surfaced on the Internet in October 1993[4]. It was not until 1999, when Shawn Fanning developed the file sharing utility known as Napster, that MP3's began their explosion of popularity. After completing a beta version, Fanning posted his utility to download.com where it quickly became a popular tool. Using Peer-to-Peer (P2P) technology, Napster allowed users to remotely locate and share audio files without requiring storage of those files on a central server.

[2] Crawford, Walt
[3] MP3
[4] Ibid

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Napster promptly satisfied a desire in the Internet community. Music could now be searched for and distributed with relative ease and more importantly to some, without having to purchase a CD. In less than a year, Napster had grown from 0 to over 60 million hits a month[5] [4]. It did not take long before this excitement caught the eyes of music artists and the RIAA.

A new network emerged to address the shortcomings of the Napster network. One popular network, the Gnutella network, made possible the release of programs such as Bearshare, Gnucleus, Limewire, Morpheous, WinMX and XoloX. Napster relied upon a central repository or server, which contained a list of all the songs and the users whose hard drives stored those songs. This central list was no longer required with Gnutella allowing users to download their music with relative anonymity.

MP3 Economics

The RIAA hastily realized that the transfer of MP3's over the Internet was costing the industry enormous sums of revenue. The alarming figure of $4.2 billion annually prompted swift and direct action on the part of the artists and drove the RIAA to take legal action. Brianna LaHara pled guilty in the first of 261 separate cases filed by the RIAA against Internet users who were supposedly involved in the illegal sharing of music files. Brianna, who was only 12-years old at the time, agreed to pay $2,000 for over 1000 songs that she had allegedly shared[6]. The RIAA had hoped that a strong zero-tolerance policy to the illegal distribution of music over the Internet would send a clear message to the Internet community to cease the illegal activity.

Some artists, such as Metallica, also took the only action they saw fit and filed lawsuits against Napster. "The problem we had with Napster was that they never asked us or other artists if we wanted to participate in their business", said Metallica's drummer Lars Ulrich[7]. Metallica endured both criticism and praise for their daring efforts to stand up against music piracy. When Napster and Metallica finally settled, Metallica agreed to provide Napster with certain material from time to time. Of course, the catch was that Napster had to first create a system that could adequately address the requirement to purchase music before downloading it.

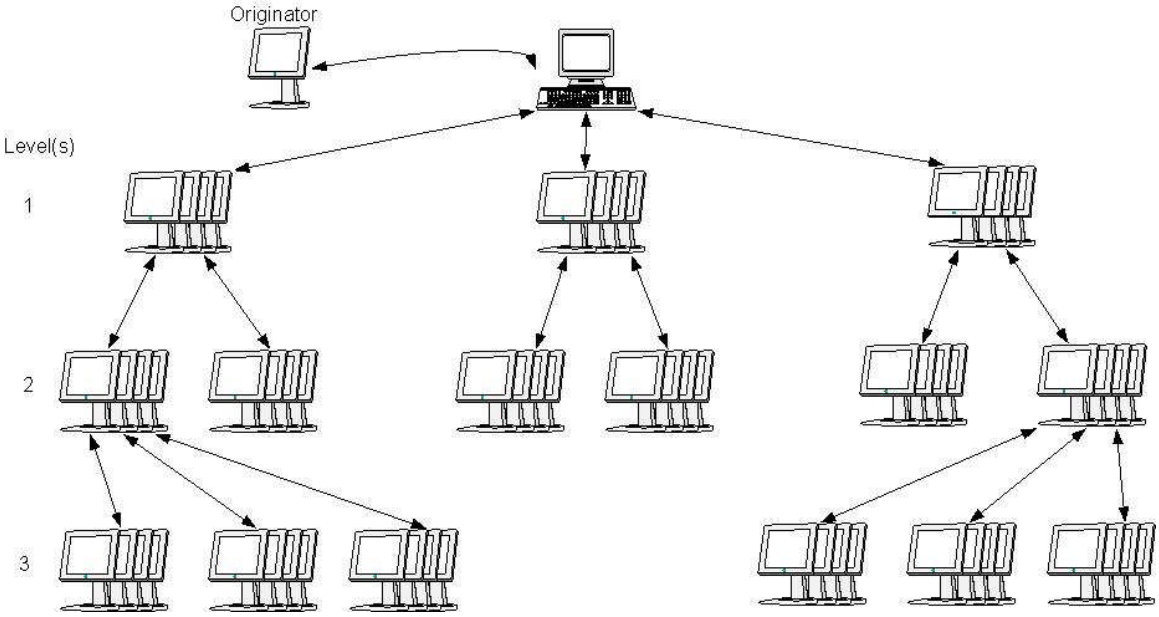
Napster adhered to the court order and removed the central database, effectively killing the entire network. The Internet community had grown accustomed to having hefty supplies of MP3's available on-demand. As the Gnutella network eliminated the need for a central database storing a list of songs with individual users, it would prove both difficult and expensive for the RIAA to track and file lawsuits against multiple organizations that developed client applications for the Gnutella network. In addition to the Gnutella network, files may also be transferred using BitTorrents, which will be described in detail later.

[5] Howstuffworks
[6] CNN.com
[7] BBC News

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Gnutella Architecture

With the absence of a central server, the Gnutella software needed a clever method of locating files searched for by the user. The solution involved configuring client software such that it was either notified or pre-programmed with the IP address of another computer on the Gnutella network. When users enter the name of a song that they desire into the search field and execute that search, the software sends a query to the known IP address. When the query is received, the local hard drive of the remote host searches for a file matching the text from the search field. If the file is present, the name of the file and the IP address are returned to the original requesting host. While that return message is being transmitted, the remote host also sends a query to all other hosts to which it is connected. Each of these additional hosts searches their respective local hard drives for a match and returns the filename along with their respective IP addresses, if a match is found. Again, while their replies are transmitted, each of those hosts queries all other hosts they are connected to. In order to prevent infinite loops, a time-to-live counter is applied limiting the number of times queries are forwarded to seven. One could imagine it as a binary tree stemming from a root node capable of searching seven layers deep, as shown in the diagram below. The tree quickly grows and is capable of reaching thousands of hosts in seconds.



These networks are advantageous to users wishing to share illicit files such as copyrighted software, MP3's or video as there is minimal logging of the file contents that are distributed. One of the caveats and severe annoyances of using client software such as Kazaa include the spyware programs that are installed in conjunction with the client opening enormous security holes.

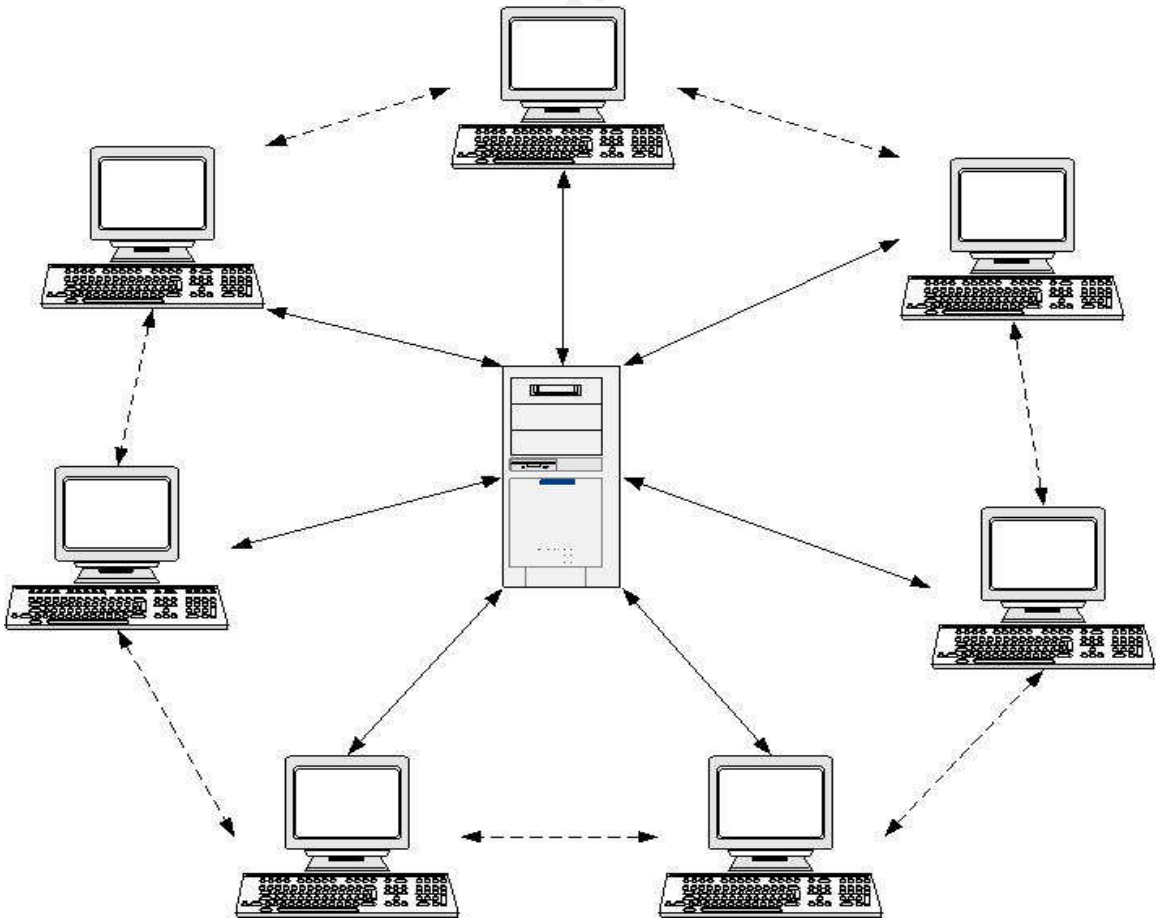
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Usenet

The Usenet has been around for a few decades, originally serving as a forum for public text based discussion. Anyone can join a discussion group and it proves very difficult to kick people out once they have joined. Utilities were developed to allow for transfer of messages across Usenet. Files are subdivided into small units of data and sent as messages through discussion groups. When an individual message was opened, it would appear as random alphanumeric characters. A reader could download the collection of messages comprising the entire file and by merging and decompressing those messages, recreate the original file. Today, many MP3's are distributed over the Usenet in this fashion.

BitTorrent

BitTorrents satisfy a niche of the Internet community and are very useful for sharing files that fall into certain categories. Bit torrents are one of the unique protocols that become more efficient as more people share the same file. Similar to the original Napster, they depend on a central database which co-ordinates the file request between originating hosts and the potential remote providing hosts. As more people come online with the same file, more hosts become



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

available to source small data slices of that file. BitTorrents also have the ability to transfer data slices before the complete file has been transferred. In other words, one can upload small slices of code to remote users while simultaneously completing the download of the same file. BitTorrents are effective for distributing new files, or more importantly, files that are in high demand. The downside to using BitTorrents is that older or less popular files tend not to be found as readily compared with using the Gnutella network.[8]

MP3 Business Case

As the popularity of the MP3 format flourished, so did the software and hardware capable of supporting it. Now anybody can download free software from the Internet, and play MP3's on their PCs. Car stereos and home entertainment systems were release that could play MP3's natively. Portable MP3 players were developed and release into the marketplace. As consumers invested in these products, it quickly became apparent there could be a profitable market in providing legal or purchased MP3's on the Internet.

Legal MP3's

"Legal MP3's" is the term commonly used to refer to music in MP3 or AAC format that has been legally obtained or generated. Obtaining a legal MP3 could be as simple process as logging on to a website that sells MP3's and purchasing the music ready for instant download and immediate playback. Steps to generating legal MP3's include purchasing a music CD and ripping it, as consumers are entitled to reproduce copies of music of which they already own. *Ripping* a CD is the act of extracting music from a CD and converting it into MP3 format. Previously software required this to be done in two steps. The two steps consisted of extracting the CD audio to .wav files followed by converting the .wav files to .mp3. Recent software extracts CD audio and converts it on the fly directly to .mp3,

Online Sources

There are many companies who have developed online websites capable of providing legal MP3's for download for the typical cost of $0.99. These sites have been active for some time now and every month an abundance of new sites come online hoping to capitalize on the growing market. Some of the more popular ones websites include the following:

iTunes (www.apple.com/iTunes)
RealNetworks

[8] Dessent, Brian

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

MP3.com
Audible.com (source for audiobooks – compatible with iTunes & iPod)
MyMusic.com

Licensing

In a competitive market place, many companies opted to develop a proprietary licensing solution. This concept pleased the recording industry as it prevented a single user from purchasing a song and then distributing it to a cast of thousands. The other advantage proprietary licensing provided was that it encouraged users to return to the same website to purchase additional music tracks.

Microsoft - Windows Media Audio

Microsoft applied Digital Rights Management (MS-DRM) to audio files stored in the Windows Media Audio (.wma) format. Microsoft's digital rights management scheme is accomplished using a variety of encryption methods including a simple block cipher and Elliptic Key Cryptography (ECC)[9]. Keys are used to verify the licensing information, or the users right to play a particular track. The audio content is decrypted by another process running on your computer and returned to Media Player during playback. Microsoft went through great lengths to ensure that all communication between various processes on local machines was encrypted. This is demonstrated as the content is played, the data passes through a decrypt-encrypt-decrypt sequence as data returns to Media Player from the decrypting process.

Apple - FairPlay

The Apple solution to capturing and preserving market share was demonstrated with the release of a system called FairPlay – Digital Rights Management (DRM). Users are only able to obtain audio that is playable on their iPods if they purchase and download it from iTunes Online Music Store (iTMS), or compatible online partner such as audible.com. FairPlay was designed to be fair to the artist, to the record companies and to users. Every track that is purchased through iTMS is encrypted with a master key that was coded using a separate random generated key. The random key is stored by Apple and is linked to each respective online user profile. In order to achieve offline playback of the music, each random key is also stored locally by iTunes in an encrypted key repository. Whenever a user desires to playback a track, the random key is used to decrypt the master key, which in turns decodes the AAC audio stream.

AAC stands for Advanced Audio Coding and was intended to be the replacement for MP3. It is an extension of MPEG-2 and was further refined in MPEG-4. The end result is that music encoded with this lossy data compression scheme yields

[9] Screamer, Beale

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

greater stability and quality than traditional MP3's at equivalent or slightly lower bit rates.[10]

All iPods have their own encrypted key repository as well. Each time a track is copied to an iPod, the random key stored in the iTunes encrypted key repository is copied over to the encrypted key repository of the iPod. This provides all the required information for the iPod to decode and playback the AAC audio stream.

Some restrictions introduced by FairPlay include the limitation of tracks to be played on a maximum of 5 authorized computers. Protected songs can be transferred to an unlimited number of iPods. All FairPlay tracks can be burned to CD an endless number of times. The resulting CD could be ripped into MP3 format, but there would be a reduction in the sound quality as the data experienced multiple compression cycles. Finally, play lists must be changed after burning to CD a set number of times, if at least one of the songs is protected using FairPlay.

Sony - ATRAC

ATRAC (Adaptive TRansform Acoustic Coding) was a standard developed by Sony in 1991. It was later enhanced in ATRAC3 and ATRAC3plus in 2000 and 2003, respectively. It is used primarily for recording audio onto MiniDiscs. The bit rate for SP mode, referred to as CD-quality mode, is recorded using 292kbps complete with separate left and right channels.[11]

RealNetwork - Helix

In January of 2004, Real announced they were creating an online music store featuring DRM-protected music in the AAC format. Helix is the player developed for playing audio on Linux and other operating systems. Real has recently become a media focus as they have reverse engineered the FairPlay licensing algorithm.[12]

Limitations of Licensing

A recent article published on CNET shows the limitation of developing proprietary keying mechanisms. The potential market place is too competitive to develop audio players that will only recognize one DRM format. Apple, Sony, Microsoft and RealNetworks are all guilty of this. Each company developed a proprietary format in which audio music could be purchased online and downloaded locally for play on PCs or portable playing devices. Obviously, it would be advantageous for an online music provider to either have the vast majority of the market share and/or have the ability to distribute audio music that could be supported by multiple vendor products. It was the latter that drove RealNetworks

[10] Wikipedia. "Advanced Audio Encoding."
[11] Wikipedia. "ATRAC."
[12] Wikipedia. "RealNetworks."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to reverse engineer the FairPlay protection technology[13], required to play audio tracks on the iPod. This accomplishment made RealNetworks the only non-apple company capable of providing audio tracks compatible with the iPod, for both Windows and Mac users.

This development has the potential to become a large battle that will wage back and forth between the two rivals as noted when Apple responded in a press release stating, "We strongly caution Real and their customers that when we update our iPod software from time to time it is highly likely that Real's Harmony technology will cease to work with current and future iPods."[14]

The Future

The desire for consumers to obtain music over the Internet will not end soon. This has become an extremely popular method of obtaining music for personal use. DRM is a valid solution to protecting the interests of artists and the recording industry in general. It allows for the legitimate purchase of MP3's using online stores. A common weakness has been identified with the use of proprietary implementations of DRM. In order for companies to remain profitable for years to come they will either have to maintain a loyal user base or invest in a non-proprietary implementation of DRM licensing. An open algorithm that stands up to public scrutiny and countless testing is the best system we have to identifying a sound keying system. The industry has already shown that if the desire is great enough, someone will evetunally crack a proprietary system, as was the case between Real and Apple.

DRM is not without its drawbacks. It is responsible for the inclusion of "unskippable track" used to play commercials where the copyright notice should appear. Another drawback includes placing copyright protection on material that is already in the public domain.[15]

One final concern is a detail that will prove extremely difficult to resolve. As long as audio requires output to be heard using a sound card or a stereo, it has the potential to be captured and recorded with no encryption. No legal action to date, on behalf of the artists or the RIAA, has seemed to slow the illegal distribution of audio music over the Internet. As long as people have the desire to circumvent licensing restrictions, chances are slim that a successful method to prevent copyright infringement and the illegal distribution of audio music over the Internet will be developed.

[13] CNET Networks, Inc. "RealNetwork Slashes Song Prices."
[14] CNET Networks, Inc. "Commentary: RealNetworks lobs another grenade."
[15] Wikipedia. "Digital Rights Management."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. BBC News. “Napster settles Metallica lawsuit.” Entertainment: New Media. 13 Jul, 2001. URL: http://news.bbc.co.uk/2/hi/entertainment/1436796.stm. (18 Aug. 2004).

2. CNET Networks, Inc. “Commentary: RealNetworks lobs another grenade.” 17 Aug. 2004. URL: http://news.com.com/Commentary%3A+RealNetworks+lobs+another+grenade/2030-1069_3-5313016.html?part=rss&tag=5313016&subj=news.1069.20. (17 Aug. 2004).

3. CNET Networks, Inc. “RealNetwork Slashes Song Prices.” 17 Aug. 2004. URL: http://news.com.com/RealNetworks+slashes+song+prices/2100-1027_3-5312143.html?part=rss&tag=5312143&subj=news.1027.20. (17 Aug. 2004).

4. CNN.com. “12-year-old settles music swap lawsuit.” Technology. 18 Feb 2004. URL: http://www.cnn.com/2003/TECH/internet/09/09/music.swap.settlement/. (18 Aug. 2004).

5. Crawford, Walt. “MP3 and CD-Quality Sound: The Laws of Physics have Not Been Repealed.” 1999. URL: http://home.att.net/~wcc.techx/MP3.htm. (16 Aug. 2004).

6. Dessent, Brian. “Brian’s BitTorrent FAQ and Guide.” (10 May 2003). URL: http://dessent.net/btfaq/. (17 Aug. 2004).

7. “MP3.” URL: http://www.wordiq.com/definition/Mp3. (16 Aug. 2004).

8. Howstuffworks. “How File Sharing Works.” 2004. URL: http://computer.howstuffworks.com/file-sharing.htm. (16 Aug. 2004).

9. Recording Industry Association of America. “Anti Piracy.” 2003. URL: http://www.riaa.com/issues/piracy/default.asp. (18 Aug. 2004).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

10. Screamer, Beale. “Microsoft’s Digital Rights Management Scheme – Technical Details.” URL: http://www.spinnaker.com/crypt/drm/freeme/Technical. (17 Aug. 2004).

11. Wikipedia. “Advanced Audio Encoding.” URL: http://en.wikipedia.org/wiki/Advanced_Audio_Coding. (17 Aug 2004).

12. Wikipedia. “ATRAC.” URL: http://en.wikipedia.org/wiki/ATRAC. (17 Aug 2004).

13. Wikipedia. “Digital Rights Management.” URL: http://en.wikipedia.org/wiki/Digital_rights_management#DRM_advocates. (19 Aug 2004).

14. Wikipedia. “RealNetworks.” URL: http://en.wikipedia.org/wiki/RealNetworks. (17 Aug. 2004).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event