An Analysis of Security Vulnerabilities in the Movie Production and Distribution Process

Simon Byers
180 Park Ave
AT&T Labs – Research
Florham Park, NJ
Email: *byers@research.att.com*
Phone: (973) 360-8283
Fax: (973) 360-8077

Lorrie Faith Cranor
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
Email: *lorrie@cs.cmu.edu*
Phone: (412) 268-7534
Fax: (412) 268-7287

Eric Cronin
CIS Department
University of Pennsylvania
Philadelphia, PA
Email: *ecronin@cis.upenn.edu*
Phone: (215) 732-6395

Dave Korman
A230 180 Park Ave
AT&T Labs – Research
Florham Park, NJ
Email: *davek@research.att.com*
Phone: (973) 360-8368

Patrick McDaniel
A230
180 Park Ave
AT&T Labs – Research
Florham Park, NJ
Email: *pdmcdan@research.att.com*
Phone: (973) 360-5721
Fax: (973) 360-8970

Abstract

Unauthorized copying of movies is a major concern for the motion picture industry. While unauthorized copies of movies have been distributed via portable physical media for some time, low-cost, high-bandwidth Internet connections and peer-to-peer file sharing networks provide highly efficient distribution media. Many movies are showing up on file sharing networks shortly after, and in some cases prior to, theatrical release. It has been argued that the availability of unauthorized copies directly affects theater attendance and DVD sales, and hence represents a major financial threat to the movie industry. Our research attempts to determine the source of unauthorized copies by studying the availability and characteristics of recent popular movies in file sharing networks. We developed a data set of 312 popular movies and located one or more samples of 183 of these movies on file sharing networks, for a total of 285 movie samples. 77% of these samples appear to have been leaked by industry insiders. Most of our samples appeared on file sharing networks prior to their official consumer DVD release date. Indeed, of the movies that had been released on DVD as of the time of our study, only 5% first appeared after their DVD release date on a web site that indexes file sharing networks, indicating that consumer DVD copying currently represents a relatively minor factor compared with insider leaks. We perform a brief analysis of the movie production and distribution process and identify potential security vulnerabilities that may lead to unauthorized copies becoming available to those who may wish to redistribute them. Finally, we offer recommendations for reducing security vulnerabilities in the movie production and distribution process.

1 Introduction

The U.S. motion picture industry estimates that its revenue losses due to unauthorized copying and redistribution of movies via physical media (video cassettes, DVDs, VCDs etc.) exceeds $3 billion annually (Motion Picture Association of America, 2003).[1] Each year over 400 facilities for illegally duplicating audiovisual content are discovered in the U.S., and many more are believed to remain undiscovered in both the U.S. and overseas (Serafini, 2003). In 2001, 74 such facilities were raided in Asia (Valenti, 2002). Malaysia, Pakistan, and China are believed to be among the largest producers of unauthorized copies of audiovisual content. The movie industry has not released estimates of revenue losses due to Internet redistribution of unauthorized copies; however, recent studies have estimated that there are 350,000 to 400,000 illegal movie downloads each day and projected revenue loses of up to $4 billion annually within the next two years (Deloitte and Touche, 2003; Wray, 2003).

Estimating revenue losses due to illegal downloads is problematic because it is difficult to determine what fraction of illegal downloads result in lost revenue for the industry and whether illegal downloads, through the "free publicity" they generate, have any positive impacts on box office revenues. Nonetheless, it is likely that redistribution of unauthorized copies via the Internet will increasingly affect DVD movie sales and paid Internet distribution of movies. As the ease of downloading unauthorized copies of movies grows with the availability of low-cost, high-bandwidth Internet connections and peer-to-peer file sharing networks, the movie industry's concerns about illegal downloads is intensifying. These concerns are heightened by unauthorized copies of movies becoming available on the Internet prior to their U.S. theater release (Seiler & Snider, 2003).

Much of the discussion about preventing unauthorized copying of movies has focused on shutting down the mass production and distribution of pirated movies and on schemes to prevent consumers from making unauthorized copies of movies from DVDs, VCDs, paid Internet downloads, or digital television broadcasts (Valenti, 2002). Until recently, there was little public discussion about security measures to prevent unauthorized copies of movies from falling into the hands of those who will mass produce them—sometimes before their theatrical release. In a recent interview with *The Guardian*, one industry watcher, Mark Endemano, director of Deloitte Consulting's media practice, criticized the movie industry for concentrating on bootleg DVDs and video cassettes (Wray, 2003). In a *Wall Street Journal* interview, Walt Disney Studios chief Dick Cook criticized the common industry practice of sending out thousands of screener DVDs to Academy voters, saying that the industry had been slow to acknowledge that this practice was facilitating movie piracy. "The unfortunate part of this industry sometimes is that it has to get hit over the head before something happens," he said (Mathews, Orwall, & Chen, 2003).

In the Spring of 2003 several press reports highlighted security measures that movie studios were putting in place to prevent unauthorized copying of movies during the pre-screenings conducted for the media or as part of marketing research (Eller & Cieply, 2003; Rea, 2003; Seiler & Snider, 2003). Despite these measures, some movies are becoming available on the Internet before their theatrical release, and in some cases before a movie has been fully edited. For example, an early version of Universal's *The Hulk* began circulating on the Internet two weeks before its June 20, 2003 U.S. theater release date (see Figure 1). The version illegally released on the Internet had incomplete computer graphics, which were widely criticized on Internet message boards (Haberman, 2003a). Within three weeks Kerry Gonzalez was charged with posting the purloined film on the Internet. Gonzalez reportedly obtained a video tape of a pre-release "work print" of the movie from a friend, who had in turn received it from an employee of a Manhattan print advertising firm that was promoting the movie. He plead guilty to a single count of felony copyright infringement and was sentenced to six months' house arrest and three years' probation. Universal told the court that the incident had cost the studio $66 million (Graham, 2003; Haberman, 2003b; McClam, 2003; Reuters, 2003).

Our research attempts to classify the sources of unauthorized Internet copies of movies that were in the U.S. box office top 50 during an 18-month period beginning in January 2002. Much unsubstantiated debate has occurred, but we know of no reliable data on this subject in the public domain. In this paper we present a brief analysis of the movie production and distribution process and identify security vulnerabilities that may lead to unauthorized copies of movies becoming available to those who may wish to redistribute them. We present our analysis of time lags between Internet, theater, and DVD releases during our study period. We describe our methodology for determining the probable source of Internet copies and the results of our analysis. Finally, we offer recommendations for reducing security vulnerabilities in the movie production and distribution process.

2 Movie Production and Distribution

Our examination of security vulnerabilities begins with the movie *production* process, in which various audio, video, and digital artifacts are created and combined into the finished product. We then examine the movie *distribution* process, which includes the physical or electronic distribution of movies to consumers as well as to critics, awards judges, and others. Marketing and related activities may occur during both the production and distribution processes.

Figure 2 describes one possible production and distribution workflow. Note that this is but one model of the production environment. Each studio has a unique set of tasks and participants, but we believe that most studios' processes include almost all of those shown here. While our analysis is driven by this workflow, it is not dependent on the particular details of this structure.

The nexus of the production process is the editing room. This is the place where the film is assembled by cutting and mixing the physical location video and audio recordings (shots). Once rough cuts of these shots are available, additional aspects such as computer generated special effects (FX) and music and sound synthesis (aud) are added by outside parties. In all cases, the enhanced content is returned to the editing room, possibly for further cutting, modification, and enhancement. Finally in the post-production stage, the visual and audio elements of a movie are fine-tuned. As with most of the other parts of the production process, post-production may be outsourced to other companies.

Parallel to the development of the content itself are related business activities. Marketing departments develop advertisements to promote the movie, often long before the content is actually completed. Trailers and posters are created to raise awareness of the movie. The marketing department also gauges audience reaction to early cuts of the movie shown in private focus group screenings. The film is altered in response to audience reaction and surveys. Often when the content is nearing completion, studio executives and financial backers view the content and make suggestions. The final version to be shown in theaters is completed when the editors, directors, producers, and marketing department are satisfied.

The distribution process replicates and delivers the final version to authorized parties. Of key interest to us is the timing of delivery to the various participants. We consider three distinct periods: prior to theater release, between theater release and DVD release, and after DVD release.[2] This last phase, after DVD release, represents an opportunity for end consumers to make unauthorized copies (e.g., by directly *ripping* the content from purchased DVDs).

Prior to theater release, the final version may be distributed to many parties. Critics and awards judges may receive copies. Note that this process serves an essential function in the movie industry: to publicize and draw (hopefully positive) commentary about the movie. However, the sheer number of people involved at this stage considerably complicates content security. Many studio employees have access to the final version: marketing and executives continue to view the content and build and execute strategies for its promotion. The content is typically delivered in some portable format (VHS or DVD) to all these parties.

The content itself must be replicated by a film production facility, where any number of employees may have access to it. On or immediately prior to the release date, the content is delivered to the cinema. Historically, movie releases have been staggered across locations. However, because of concerns about unauthorized copying, some studios are compressing their release time frames (Rea, 2003; Seiler & Snider, 2003). Once a cinema receives a movie, it becomes accessible to cinema employees. When a movie is projected it is exposed to members of the public who may make unauthorized copies of the projected image as well as to cinema employees who have direct access to the projector.

Several months after theater release, movies are replicated on DVDs at DVD pressing plants. DVDs are then distributed to stores and movie rental companies. It is not unusual for U.S. DVD distribution to begin a month or more before the official DVD release date. (Typically, overseas DVD distribution of American movies does not begin until after the U.S. release date.) Thus, store employees may have access to DVDs several weeks before their release, and in some cases, stores may begin selling DVDs prior to the release date contrary to studio policy.[3]

3 Security Vulnerabilities

A variety of attacks against movie content production and delivery systems are already proving successful. In studying these attacks we make the critical distinction between *insider* and *outsider* attacks (Neumann, 1995). In general, insiders are members of the (at least partially) trusted community. As is true of information security more generally, most of the precautions and countermeasures used to address insider threats in the movie industry are necessarily different than those that address outsider threats.

Insider attacks can be extremely difficult to protect against. As an example we take the case of Robert Hanssen, who managed to pass large amounts of sensitive FBI data to the Russians. The FBI presumably takes strong measures against exactly such an insider attack. Yet Hanssen was incredibly successful in his attack against FBI protected content. On the whole though, despite the seeming difficulty of preventing insider attacks, an organization can wield considerable power against insiders and impose strong constraints on how insiders conduct their legitimate affairs. In contrast, many organizations (including the FBI) have very weak control over outsiders. Prevention of outsider attacks is often a wasted effort when strong measures are not first put in place to prevent insider attacks.

3.1 Insider attacks

Our analysis reveals many types of potential insider attacks on the movie production and distribution process. The following lists but a few of the many potential threats to secure movie production and distribution:

- Unauthorized copying of a movie in the editing room or nearby in the supply chain, whether first cut or final product. These copies often have small differences from the released version or include incomplete audio or visuals, as shown in Figure 3. Some are marked with obtrusive text that identifies their source, as shown in Figure 4, or include on-screen counters, as shown in Figure 5.
- Unauthorized copying of a critic's advanced copy of a movie. This may have the text "Screener copy only, property of *some name*" appearing on the screen occasionally, as shown in Figure 6.
- Unauthorized copying of a promotional or preview screening copy. This may be marked in a similar fashion to critics' versions, as shown in Figure 8.
- Unauthorized copying of an awards judge presentation of a movie. Copies may be marked with the text "For your consideration," as shown in Figure 7.
- Digital through-the-air video recording by a projectionist at a cinema with aspect-correct video, suitable exposure, and direct audio. These copies have highly variable video quality, but often can be very good.
- Unauthorized copying of a consumer medium such as DVD or VHS at the factory or any other point prior to sale. These copies are unmarked and of near perfect quality.

Note that we consider all participants in the movie production and distribution process other than the end consumer to be insiders, although some are not employed directly by movie studios.

3.2 Outsider attacks

For comparison we also show some examples of outsider attacks:

- Digital through-the-air video recording by a consumer using a camcorder from a cinema seat. These copies generally have bad video and audio quality due to the through-the-air nature of the acquisition. Often it is noticeable that the copy was not recorded at the same angle from which it was projected, as shown in Figure 9.
- Unauthorized copying of a consumer rental DVD or VHS tape. These copies (and the following two types) can be near perfect in quality but do not appear until some time after the creation and release of the content.

- Unauthorized copying of a consumer purchased DVD or VHS tape.
- Unauthorized copying from cable, satellite, or broadcast TV.

Outsider attacks seemingly represent a greater threat due to the much larger number of potential attackers and the fact that these attacks occur when the movie is in final form and is free from studio markings. However, in the next section we examine some important attributes of these copies that can override these concerns.

3.3 Freshness and quality

Unauthorized copies can vary in many ways, two of which are of particular importance: freshness and quality. A film's freshness depends on how new it is: a film is most fresh at or prior to its theatrical release. Freshness is important because demand tends to be highest for new movies and marketing efforts are greatest for recent releases. Unauthorized copies of movies that have not yet been released in theaters or in a particular market are especially valued because they are viewable before a movie is available through legitimate channels.

The path that unauthorized copies flow through may result in copies not becoming widely available when they are very fresh. For example, unauthorized copies may be distributed initially in relatively closed communities via FTP sites, IRC channels, or internal university servers, and only later emerge onto full scale peer-to-peer file sharing systems. Ultimately, unauthorized copies may be indexed by content verification sites, making the copies widely accessible. Content verification sites act as indexes for movies shared on peer-to-peer networks, providing information such as file names, date of first appearance (on the verification site), file size, checksum,[4] and quality. The time it takes an unauthorized copy to make its way into an index may range from one day to several weeks or more.

Content quality is also of prime importance. Due to the size of files required to hold a digital representation of a movie, aggressive video compression is often employed. For example, a 1.5 hour film can be as large as 4.7 gigabytes at full DVD quality and is usually compressed to one or more 700 megabyte files for Internet distribution. Degraded quality due to lossy video compression coupled with quality problems introduced by the copying method (for example, through-the-air capture) can result in poor quality copies that are not satisfying to end consumers. On the other hand, high-quality unauthorized copies may be indistinguishable or nearly indistinguishable from legal copies distributed via portable media or TV broadcast.

There is considerable desire for movies that are both fresh and of high quality. (We note that in the music arena freshness and quality play a different role due to differences in the marketing and usage of the media, the files sizes involved, and fundamental differences between audio and video.) Generally, unauthorized copies with these characteristics can be obtained only through insider attacks. Fresh (before or during cinema release), good quality copies (TV quality or better) are almost impossible to obtain through an outsider attack. This observation is of key importance to our analysis of movie production and distribution security vulnerabilities. The number of holes to be plugged in preventing insider attacks is miniscule compared to those required to prevent acquisition and re-transmission of outsider originated copies. Moreover, the people involved in insider attacks are by definition under some influence of the content owners in that they have jobs in the industry and have something to lose. This has important implications for preventing unauthorized copying of movies.

4 Empirical Analysis

In order to gain additional insights into the source of leaked movies, we conducted an empirical analysis of movies that were in the U.S. box office top 50 between January 1, 2002 and June 27, 2003. This section describes our methodology and the results of our analysis.

4.1 Methodology

We developed our data collection procedure with the following requirements in mind:

- It must be documented and reproducible.
- An analysis that requires only publicly available data is preferable over one that requires privileged access. Clearly such analyses are also more reproducible.
- It should be consistent with fair use provisions of U.S. Copyright Law.
- It should be automatable to the extent that both ongoing study and bulk retrospective analyses can be performed.

Our methodology was also influenced by the modest resources we had available to us for this project. We expect that the movie industry could devote significantly more resources to conducting a similar study, given the economic consequences of this issue for them.

4.1.1 Movie Data Set

We developed a suite of programs that access publicly available movie web sites and compile lists of movies that were in the U.S. box office top 50 any time between January 1, 2002 and June 27, 2003. This process automatically collects and organizes a variety of data including cinema release date, DVD release date, distributor, MPAA rating, box office take, and some crude popular ratings. We gathered statistics on 409 movies that met our criteria. We removed from our data set those movies that were released outside the U.S. prior to their U.S. release, including those screened at foreign film festivals prior to U.S. release. We also removed several movies from our data set that we had incomplete information about. Our resulting data set includes 312 movies.

4.1.2 Unauthorized Copy Identification

For each movie in our data set we used our software to search an online content verification site and automatically find all the unauthorized copies. The information on content verification sites is posted and maintained by volunteers, and may not be completely accurate. Furthermore, there is often a delay of several days to a few weeks from the time a movie is first made available on a peer-to-peer network until it is indexed on a content verification site. However, use of the content verification site allowed us to obtain data for movies posted over more than an 18 month period without monitoring the peer-to-peer network for that entire period. In addition, it allowed us to avoid downloading files that do not contain the content they claim to contain (often referred to as decoys).

Some of the movies we queried on the content verification site resulted in no hits, others resulted in multiple hits (indicating that multiple versions of a particular movie were available on a peer-to-peer network). We limited our search to a single content verification site; querying multiple content verification sites would likely have produced more hits. The content verification site we used usually does not index poor quality copies of movies.

4.1.3 File Sample Acquisition

Using the information obtained from the content verification site, we located the corresponding files on a peer-to-peer network automatically and acquired a small part of each relevant copy (on average, about five percent of each movie).[5] We were unable to download the files corresponding to a few of the relevant hits, and 27 of the files we downloaded were unplayable. We also discovered that 18 files were foreign releases (for example, with non-English subtitles), and we did not consider those further. We successfully downloaded and played files corresponding to 285 relevant hits for the 312 movies we studied. These hits referenced online copies of 183 movies (59% of the movies in our data set).

We wrote a Perl module to provide a convenient interface to a peer-to-peer client running on a 200 MHz computer connected to the Internet via cable modem. The module allowed us to initiate, monitor, pause, and cancel file downloads in such a way as to end up with a sample of any required size of each of the desired files. It took approximately one week to acquire 285 playable samples, totaling over 18 gigabytes of data.

4.1.4 Content Classification

Once the samples were acquired an automated script served the samples to a pool of human observers for judgment, along with a form in which to enter various data. The data recorded included a judgment on video and audio quality along with the presence or absence of the various possible features of unauthorized copies. Some automated analysis methods were performed also at this stage. In most cases it was straightforward for the observers to judge the audio and video quality. However, there were 38 samples for which observers commented on their forms that they were not entirely sure that their judgments were correct. In most cases their uncertainty was about audio quality.[6]

It should be noted that some of the samples may have had studio-inserted text tags indicative of a critic release or other pre-release that were removed before the movie was posted to the Internet. If the text is inserted only at the beginning and not superimposed on the movie content, it is particularly easy to remove. We found one sample where someone had attempted to remove this text but appeared to have inadvertently left one frame in the version they posted to the Internet. We suspect that many of our other samples had the studio text removed completely.

4.1.5 Analysis

Based upon the data collected in the above processes we examined the interaction between freshness, copy quality, and attack point. For each movie we calculated the time lag between its theater release and its first appearance on the content verification site. If the movie had been released on DVD we also calculated the time lag between the DVD release date and its first appearance on the content verification site.

We classified the attack point as insider (as opposed to outsider) if any one of the following conditions are met:

- If the copy appearance date is prior to cinema release.
- If the copy has editing room artifacts such as frequent boom microphones in shot or is obviously not the final released edit (see Figure 3 for examples).
- If the copy has any industry related text or overt watermarks (see Figures 4, 5, 6, and 8, for examples).
- If the copy has good though-air video capture but apparently direct captured audio and appeared before DVD/VHS release date. In this case a cinema employee likely captured the audio directly from the projector and captured the video via a camcorder positioned in the projection booth or in an optimally located cinema seat.
- If the copy is plainly made from DVD source and appeared before DVD release date (likewise for VHS).

Other copies are classified as outsider sourced or unknown.

4.1.6 Limitations

Our analysis provides some much-needed empirical data; however, it is important to be aware of some of the limitations inherent in our methodology. First, no analysis of this type will ever be able to access all or even nearly all distinct unauthorized copies of movies. Hence we inherently underestimate the number of such copies in existence. Our usage of content verification sites to determine when each movie became available on the Internet is a key idea that permits retrospective analysis, allowing us to avoid a lengthy data collection process. These sites also relieve us of much of the load of decoy removal, but can introduce other errors. Specifically they result in estimates for the appearance time of files on the Internet that are somewhat later than they should be. Thus, our estimates of the number of insider copies are conservative. Furthermore, the content verification site we used appears to remove entries for particularly poor copies, which are often posted earlier than higher-quality copies, adding some bias to our analysis. From our experience reviewing the study samples, the content verification sites appear to be otherwise very accurate. Our spot checking of release dates against other data sources revealed occasional minor discrepancies such as inconsistent reporting of limited and wide release dates, but these errors were rare and not very significant. We did not find any movies in our sample that appeared to be decoys.

Our copy sampling and viewing procedure may introduce some additional errors. We were unable to view 27 of the samples we downloaded. While it is possible that some of these samples were corrupted, we suspect that most were encoded in formats that were unplayable when only a small sample was obtained. In addition, because a movie with insider markings may not have these markings in every frame, the insider markings may not appear in the short sample of each movie that we viewed, causing us to undercount the number of copies with such markings. Also, some samples may have had insider markings removed before they were posted to the Internet. Again, this results in an overly conservative estimate of insider leaks.

The one area where we may not be conservative is in our estimates of insider leaks of unmarked DVD-quality copies. Some of these copies that appear in the weeks prior to official consumer DVD release may have been purchased by consumers from stores that made them available prior to the release date.

It should also be noted that our study focused on popular movies. It is not clear whether we would find similar patterns for small, independent movies.

4.2 Results

Of the 312 movies we studied, 183 were indexed on the content verification site, indicating widespread Internet availability. Of the 285 movie samples we examined, 77% appear to have been leaked originally by industry insiders (determined using the criteria we outlined in section 4.1.5). On average, the movie samples we examined were indexed 100 days after theater release and 83 days before DVD release. While only 7 of these movies were indexed prior to their theater release date, 163 were indexed prior to their DVD release date. Only 5% of the movies we studied that had been released on DVD as of the time of our study were first indexed after their DVD release date, indicating that consumer DVD copying currently represents a relatively minor factor compared with insider leaks.

Figures 10 and 11 illustrate the distribution of time lags between appearance on the content verification site and theater and DVD release, respectively. The graphs show that many movies appear on the Internet within three weeks of their theater release date. These include movies leaked during the production and cinema distribution process as well as copies sent to critics and Oscar reviewers. A second wave of leaks begins about one month before DVD release. Most of those leaks likely originate from DVD pressing plants, DVD distributors, retail employees, or Oscar reviewers; however, some may occur as a result of consumer copying of DVDs purchased at stores that sell them before their official release date.

The vast majority of the samples in our data set were DVD quality. Those that were not DVD quality had shorter lag times between their theater release and Internet availability. Likewise, those with overt watermarks or textual markers also had shorter lag times. Table 1 shows the classifications of the movies in our data set along with the average lag times for each classification. Note that we have multiple samples for about half of the movies in our data set, for example both a through-the-air quality sample and a DVD quality sample.

The percentage of movies indexed on the content verification site and the mean lag times varied considerably between movie studios. The production and distribution processes of each studio may account for some of this variation, as well the types of movies produced. We were unable to find a correlation between average lag times and average box office take for each studio, however. Table 2 shows the data we collected for each studio with five or more movies in our data set. Note that in some cases movies are listed as being released by a studio that is a division of a larger movie production company. Thus, for example, Walt Disney movies in our sample may be classified as being released by Buena Vista Pictures or Touchstone Pictures.

5 Current and Recommended Security Measures

The movie industry has been taking steps to identify and shut down illegal video reproduction facilities and stop the distribution of pirated videos and DVDs for some time (Serafini, 2003; Valenti, 2002). However, until recently, there were few public reports of industry steps to prevent individuals from obtaining the first unauthorized copy from which many other copies might be reproduced. We refer to this first unauthorized copy as a *leaked* copy, and view the prevention of leaks to be paramount in preventing unauthorized reproduction of fresh, high quality copies of movies. Leaked copies are of particular concern to the movie industry because they make it possible for illegal copies of movies to be reproduced widely before a theatrical release. Fortunately, leak prevention is, perhaps, the security area where the industry can most easily exert control.

In the following subsections we first review known steps the movie industry is currently taking to prevent leaks and then consider additional countermeasures appropriate in three distinct phases: short, medium, and long term. The short term solutions are intended to suggest immediate and simple actions to prevent leaks. The medium term solutions apply existing technology, but require both modification of the content delivery processes and development of technical solutions. The long term solutions depend on the advancement of content management technologies, and hence are contingent on some factors outside the movie industry's direct control. Our proposed solutions are broad recommendations. Each production facility should perform considerable self-examination about how they handle content to best limit the possibility of leaks. Where this leads to new internal procedures and technologies, it is likely to be successful. If new measures attempt only to modify the behavior of outsiders, the effort is likely to fail.

5.1 Current Leak Prevention Efforts

The following overview of current leak prevention efforts was developed after researching news reports of movie industry security measures. Of course, it is likely that the industry is also pursuing other security measures that they have not publicized.

The MPAA is reportedly working on best practices recommendations to assist movie studios in combating piracy (Eller & Cieply, 2003). According to insiders we spoke with, the studios have followed security procedures for some time such as coding pre-release copies and requiring that all pre-release copies be signed out when they leave the studio. However, these procedures are often insufficient for preventing leaks.

Pre-release copies of movies are typically marked with anti-piracy messages and in some cases watermarks or overt textual markings that may be useful in identifying the source of an unauthorized copy. The pre-release copy of *The Hulk* that was posted to the Internet contained unique security tags on the bottom right corner of the screen, as shown in Figure 1. Although Gonzalez used software to black out the security tags before posting the film to the Internet, studio officials were reportedly able to identify the source of the leak from the remnants of these tags. The FBI was also able to track the uploaded copy to Gonzalez through his Internet Service Provider. Industry officials are hoping that the felony indictment against Gonzalez will send a strong message to others who are considering leaking movies to the Internet (Huffstutter, 2003).

Because Oscar screeners are often a source of fresh high-quality leaks, Walt Disney Studios sent screeners on video rather than DVD last year for movies such as *25th Hour* and *Treasure Planet* that were not scheduled to come out on DVD for some time. This appears to be an unusual step (Mathews et al., 2003); however, in this case it appears to have prevented the screeners from being leaked and widely distributed on the Internet. The samples of these movies in our data set appear to be unmarked DVD copies leaked during the DVD production or distribution process (appearing on the content verification site 27 and 37 days before their respective DVD release dates).

Some studios have begun using metal detectors and employing security guards equipped with night-vision goggles and binoculars at their pre-release screenings. In addition, electronic devices, including cell phones, have been banned from these screenings. Such measures were reportedly used at pre-release screenings of the Warner Brothers movies *Dreamcatcher* and *The Matrix Reloaded*; the Disney movies *The Lizzie McGuire Movie* and *Finding Nemo*; the Sony Pictures movie *Anger Management*; the Paramount Pictures movie *The Italian Job*; and the 20th Century Fox movies *Daredevil* and *Down With Love*. Of these movies, only *Dreamcatcher*, *The Matrix Reloaded*, *Daredevil*, and *Finding Nemo* appear to have been leaked to the Internet near their theater release dates (these movies first appeared on the content verification site 6, 1, 3, and 1 days after their respective theater release dates, indicating that they may have been leaked just prior to theater release). The first three samples appear to be very good camcorder copies, possibly with directly-recorded audio tracks. They may have been recorded during a pre-release screening or during a public cinema screening after release. However, the high audio quality suggests the possibility that they were leaked by a cinema employee. The *Finding Nemo* sample was reportedly a poor camcorder copy that was removed from the content verification site's database prior to our study because its quality was deemed unsatisfactory. Fox and Sony Pictures have reportedly caught individuals using camcorders at some of their screenings. In April 2003, federal prosecutors in Los Angeles charged a man with recording movies at critic screenings using a camcorder. He reportedly had a lucrative business selling pirated videos that he reproduced on 11 VHS recorders in his home. According to a press interview with Ken Jacobsen, the MPAA's senior vice president and director of worldwide anti-piracy, the MPAA has determined that 28 movies that became available illegally before their U.S. theatrical release between May 2002 and March 2003 were recorded with a camcorder at a pre-release screening (Butler, 2003; Eller & Cieply, 2003; Rea, 2003; Seiler & Snider, 2003).

Some studios have reportedly started using messengers to hand-deliver prints of popular movies with phony labels to theaters. However, according to a *USA Today* article, some of these prints are disappearing despite this measure. In addition, some studios have cut down on their use of test-market screenings in order to prevent leaks. For example, Sony prohibited test-market screenings of *Men in Black 2*, despite the director's objections (Seiler & Snider, 2003). This precaution may have prevented a pre-release leak, as *Men in Black 2* did not appear on the content verification site until 126 days after its theater release.

Because the demand for unauthorized copies is often extremely high during periods when a movie is available only in certain countries, some studios are changing their release strategies to reduce or eliminate time lags between movie openings in different countries. For example, Fox released *X2* simultaneously in 58 countries and Warner Brothers released *The Matrix Reloaded* nearly worldwide within a nine-day period instead of over a more typical release period of several months (Rea, 2003; Seiler & Snider, 2003).

A number of technical approaches to preventing leaks are also being pursued. In 2000, Macrovision received a patent on a method for preventing through-the-air capture of projected movies by superimposing infra red images on the visual image.[7] These images are not detectable to the theater audience, but show up on video captured by most camcorders. The Sarnoff Corporation and Cinea are developing a digital movie encoding designed to confuse camcorders without being detectable by human viewers. Work on this project is being partially funded by a two-year grant from the National Institute of Standards and Technology (NIST) (Cinea, 2003b; McCarthy, 2002).[8] Cinea also has developed a secure digital movie distribution system that includes encryption and auditing schemes (Cinea, 2003a). However, digital projection is not expected to come to most cinemas for some time to come due to concerns about equipment cost and projection quality. Furthermore, while digital distribution has cost-saving and anti-piracy benefits for movie studios, theater owners see little benefit from making a substantial investment in digital projection equipment. Studios may need to subsidize the purchase of digital projection equipment if they expect to see it adopted in the near future (Associated Press, 2000; Taub, 2003).

5.2 Short-term Mitigation

The movie industry has already begun to address the vulnerabilities inherent in the current workflow. While increased physical security at screenings, watermarking and other technologies are laudable and often effective, they fail fundamentally to address insider threats. There is an implicit assumption that all employees of the studio and production and distribution services are *trusted*. Any misbehavior of a single employee can nullify all the best practices and well placed trust throughout the content distribution process.

We believe that the movie industry should treat movie content in the same way the Federal Bureau of Investigation (FBI) treats sensitive intelligence and evidence. In these cases, the FBI establishes a *chain of custody* for sensitive artifacts. This defines a procedure for tracking where the artifact is at all times, as well as who is responsible for it. Obviously, this has enormous value as a forensic tool when something goes wrong (e.g., determining responsibility). More importantly, if consistently applied, this mitigates loss and exposure by clearly indicating who is responsible for the artifact at all times (i.e., overnight, in transit).

Particularly during production, many current security problems can be traced to the chaotic workflow. Policy must be developed that clearly delineates the process by which content is obtained or accessed, who is authorized to view or access it, and how failures in the process are reported. This policy, among other things, would codify the chain of custody. We expect that the MPAA's best practices work will go a long way toward this goal, but we caution that general best practices guidelines cannot take into consideration all aspects of each individual studio's operation.

Much of current content production and distribution is performed through modular and parallel processes. These simultaneous processes involve many different entities, and hence complicate content control. Adopting the physical control practices of intelligence agencies used in similar environments will help prevent future leakage (e.g., as applied by the FBI in large, coordinated investigations). One such practice would limit content exposure to only that which is strictly necessary to produce and distribute the movie. Known in the computer security community as the *principle of least privilege,* this practice exposes only as much of the content at each stage of the process as is strictly necessary for that process to be successfully executed. For example, the creators of the digital effects only need those parts of a movie that they are going to augment. If universally applied, this would greatly limit the number of entities that would have access to a complete copy of the content at *any* stage of development.

To illustrate the definition and use of policy, consider the content used by an audio production facility. A rough cut of the content is often played back to musicians while the background music is created. This helps musicians adjust their performance in response to the content imagery, and is essential to establishing auditory and visual continuity. The playback and storage of the rough-cut at the audio production facility are potential leakage channels.

One policy that may mitigate leakage in the audio production facility mandates that an appointed recipient of the content (possibly an employee of the production house) must be present during any use of the content. That person is responsible for ensuring that (a) the content is always in their immediate possession, or (b) locked in a safe that only they have access to. This simple policy, while potentially costly and cumbersome, reduces the point of vulnerability to a single person. Like any system, if the trusted part of the system (in this case, the entity guarding the movie) becomes compromised, all is lost.

A second policy would define the environments in which the content could be used. For example, the policy would mandate that screenings must be held in private screening rooms with guards. The studios have made considerable progress in the physical security of screenings. While preliminary, anecdotal evidence suggests that these techniques are somewhat successful in preventing camcorder copying, these measures must be extended to other venues as well: screenings needed for audio and CGI must be accompanied by physical control by the studios of the playback devices, pre-approved lists of the authorized personnel who may be present during viewing, etc. In addition, studios should reconsider their policy of allowing executives to check out pre-release copies for home viewing and of sending pre-release copies to investors upon their request. Once outside the studio environment, these copies may be vulnerable to unauthorized copying by many parties including family members and household employees.

Where movie production and screening activities occur entirely in the digital domain, adequate network security measures should be taken, and evidence of their completeness presented to the production managers. There should be a minimum set of security practices for any computer that will store any part of the content (e.g., physical separation from the Internet). Security audits of the networks should be commonplace. Physical measures, such as removable storage devices that are returned at the end of each work day to on-site security personnel may help prevent leakage. There is considerable experience with this kind of content management in the legal, engineering, and military manufacturing industries.

Continual vigilance is a necessary ingredient of any solution. As with any security system, having a consistent process for managing sensitive artifacts is essential. We argue that insider attacks can only be mitigated in the short term by, (a) developing sound procedures for handling content, (b) applying it uniformly to *all* employees of the production and distribution process, (c) putting in place a comprehensive infrastructure for documenting compliance with policy, and (d) auditing compliance frequently. See guidelines on both physical and computer security (Computer Emergency Response Team (CERT), 2004; Cheswick, Bellovin, & Rubin, 2003; Garfinkel & Spafford, 1996) for further detail.

Similar strategies should be applied to the distribution processes. For example, some unauthorized copying may be mitigated by reducing the number of copies sent to Oscar reviewers (Mathews et al., 2003). Our data suggests that many high quality copies are leaked from DVD pressing plants and stores. The distribution process creates many high quality authorized copies, any one of which can be leaked. Hence, the challenge is to create a process that delays, rather than prevents, leakage. Before tackling the extremely difficult problem of preventing DVD copying by consumers, it seems prudent to stop the unauthorized copying that takes place before consumers have an opportunity to buy or rent DVDs. It seems clear that more monitoring and stringent controls over DVD production facilities and distributors must be applied. Other measures, such as reducing DVD production and storage times, may further mitigate unauthorized copying.

5.3 Medium-term Mitigation

As described above, the movie industry is actively exploring the application of advanced technologies to prevent unauthorized copying. It is likely that these investigations will yield strong protections against specific threats. As is true generally in computer security, singular solutions rarely address all threats. Hence, we argue that the best way to mitigate the risk of leakage in the medium term is to combine ranges of available technologies and procedures into comprehensive solutions.

Consider the following trusted device that addresses leakage resulting from critic or awards judge content distribution.[9] Assume there is a trusted content player that provides digital or analog output appropriate for a home theater.[10] Assume further that this device is tamper resistant and has internal storage containing the content. Each device has a battery-backed internal clock. When a user (e.g., critic) wants to use the device, she must enter a time-specific key to unlock the content. Variants of one-time password schemes can be used for this purpose (Haller, 1994). To obtain the password, the user must call a operator and give the serial number of the device and content, as well as some private authenticating information (McDaniel, 2002). The user would be given the one time password which would unlock the device *for that time and allow only one playing*.

The content is stored on the device in an encrypted format. The one-time-passwords provide access to a decryption key to the player internally, but not to the user. Hence, the code is only useful for that particular playing. Moreover, stealing and breaking into the machine would yield only the encrypted content (and hence make the unencrypted content very difficult to obtain without a valid password).[11]

At playback, the player would project a one time tracking code on top of the content. This code might be an overt identifier or an invisible digital watermark (Cox, Kilian, Leighton, & Shamoon, 1997). The advantage of this approach is that not only could the user be identified in the event of leakage, but she would not have deniability (i.e. the watermark would expose the exact player, user, and time). If the user loses the authenticating information or the player, she would be responsible for contacting the central operator. Of course, the player would allow the user to cancel/pause a play-back, thus avoiding exposure resulting from a distracted user.

Note that some adversaries with video editing capabilities may be able to remove the tracking code from the content. However, removal of the code should significantly damage content quality. For example, placing a black box over or blurring out the code would create visually distracting artifacts, particularly where the code is large. The design of such codes is an open area of research and is outside the scope of this work.

The player could be made Internet accessible (and hence be continually reused for different movies). Studio personnel would push encrypted content and associated keying material over an untrusted network and into the player. Because the keys are never stored on the device, transmission of the encrypted content can be performed without additional exposure to loss.

The efficacy of the trusted player approach is crucially dependent on policy: how and when authenticating information is assigned and used will determine whether leaks are avoided. Hence, where advanced technologies are applied, the short term suggestions are still applicable, and in our minds, essential.

5.4 Long-term Mitigation

The unauthorized copying of movies is an instance of the larger problem of content control. Often cast as digital rights management (DRM) (Ramanujapuram & Ram, 1998; Gunter, Weeks, & Wright, 2001), other industries such as design and manufacturing, legal document management, and finance are currently wrestling with digital content control. The movie industry is facing a particularly daunting problem: because other industries do not directly expose their content to outsiders at any phase, much less to the public at large, the problem is somewhat more tractable for them.

The scientific community is only beginning to understand DRM. Hence, we cannot begin to predict when a solution appropriate for the movie industry is going to be available. Solutions like Microsoft's Next Generation Secure Computing Base for Windows (Corperation, 2003) provide commodity-grade DRM. However, they do not provide a level of security necessary to protect highly valuable content: the DRM-enabling hardware can be manipulated via physical attack. Hence, until such time as stronger DRM becomes available, it is incumbent on the industry to embrace currently available techniques and procedures.

We feel that it is useful to consider what (potentially unique) requirements the movie industry may place on DRM systems. There are two separate DRM systems appropriate for movie content: one for consumer users and one for the production and distribution environments. Because consumer DRM has been discussed at length in related works, we focus on the latter. The following describes a few important preliminary requirements:

- *scale* - The production and distribution workflow encompasses many different companies (sometimes on different continents), and a huge number of users. The DRM system must be able to efficiently manage this large, decentralized user community.
- *flexibility* - The production process coalesces many disparate artifacts into the finished product. Hence, the DRM solution must support complex policies that control access, duplication, and modification of content artifacts.

- *simplicity* - Any DRM solution which adds significant complexity or frustrates progress will fail. It is important that the solution seamlessly integrate with current procedures.

We are encouraged by the economics of the production and distribution process: the movie industry has enormous influence on the companies that provide services to it. Hence, it may mandate certain technologies or vendors. Such environments naturally lead to uniform (and safe) practices, and reduce the industry's exposure to leaks.

Implementing DRM only to prevent insider attacks avoids many of the concerns that have been raised about the possible mandated use of DRM in the consumer environment. For example, it avoids concerns about the ability of DRM to accommodate fair use, difficulties in managing a public key infrastructure, and the likelihood that DRM technology will be unable to prevent the distribution of content over peer-to-peer networks (Biddle, England, Peinado, & Willman, 2002; Samuelson, 2003). Furthermore, the technical challenge of implementing a system in this more controlled environment is much more tractable than the challenge of using DRM in a consumer environment. It is much easier to mandate the use of certain equipment and require individuals to participate in inconvenient authentication procedures than it would be in a consumer environment. In the event that content is leaked despite the use of a DRM system, watermarking may make it possible to precisely identify the source of an insider leak. In the more controlled environment, it may be feasible to register all individuals who are authorized to view content, and to impose overt watermarks that are easily detectable and can resist removal, but might be unacceptable to consumers. Furthermore, unlike in a consumer environment where it may be difficult to track down and punish every individual who makes an unauthorized copy,[12] insiders who are identified as the source of a leak can be fired from their jobs or have their contracts terminated, in addition to being subjected to legal action and possibly criminal prosecution.

6 Discussion and Conclusions

Our research presents the first publicly available assessment of the source of leaks of popular movies and provides a security analysis and recommendations for mitigating against future leaks. Our research suggests that the movie industry would likely benefit from implementation of some established ideas in data security; however, additional measures may be necessary in the long term. Our research suffers from the fact that we are not industry insiders nor owners of the leaked content, and our data collection was limited to information that we could obtain through public sources using modest resources. Collecting statistics on sources of leaks and performing a security analysis should be much easier for the industry than it was for us, and we assume that studios are engaged in such processes on their own.

We draw the reader's thoughts back to the Hanssen case and make the point that the movie industry ought to treat everybody within its influence equally, from studio executives and investors, down through movie editors, truck drivers and out to the critics. Such elementary procedures as audit trails of custody would seem to be in order. While we expect that this is already done to some extent, it must be applied evenly and without preference. Our study shows a large amount of insider leakage. Hence, we argue that current mitigation techniques are insufficient. Given the revenue losses claimed by the industry, spending more money and effort on internal controls is appropriate.

Movie artifacts are handled by a limited number of employees in a controlled manner during production and through much of the distribution process. In the later stages of distribution, content is handled by a large and mostly anonymous community. Securing the former environment is difficult but tractable. Securing the latter is nearly impossible. Hence, focusing efforts on insider threats addresses the most costly leakage, and represents the best opportunity for success.

Notes

[1] In some statements the MPAA has claimed this number includes only analog video cassette distribution (Valenti, 2002), while in other statements the MPAA has claimed this number covers all illegal distribution except Internet distribution (Motion Picture Association of America, 2003).

[2] There are, of course, other important events in the movie distribution process including international releases, hotel pay-per-view releases, airline releases, home pay-per-view releases, etc. Our analysis focuses only on the three periods we have outlined. In addition, some movies have separate DVD and VHS release dates; however, in our analysis we consider only the earlier of these two dates. Note that the DVD release date is the date on which a movie becomes available on DVD in the U.S. for both sale and rental.

[3] Anecdotal evidence, for example from the release of the latest Harry Potter book, suggests that book publishers have been more successful than movie studios in preventing stores from selling their products before the official release date. It might be useful to compare the strategies used by these two industries to enforce their release dates.

[4] The checksum provides an identifier for each unique copy of a movie uploaded to a peer-to-peer network. All identical copies of the same movie have the same checksum. The checksums are useful for identifying movies, and they allow for client software that can download different blocks of a movie from multiple sources simultaneously.

[5] The file sharing software we used obtains movies in blocks, usually beginning first with a block at the very end of the movie file and then proceeding with a block from the very beginning of the movie file. Since some movies are stored in multiple files, the beginning and end of the file does not always correspond to the beginning and end of the movie itself. We found that by setting our scripts to download eight percent of one file from each movie we could acquire a complete block from the beginning of most of the movies we studied. A block from the beginning of the movie is especially useful, as this is where many studio markings are found.

[6] Automated tools might be developed to more accurately assess audio quality, for example, by measuring the difference between audio channels. If little or no difference is found between audio channels, it would suggest the audio was acquired through-the-air.

[7] U.S. Patent 6018374, Method and system for preventing the off screen copying of a video or film presentation, issued January 25, 2000

[8] The NIST program that is funding this project typically funds projects that are too risky for most investors but have potential for broad economic benefits. Given the revenue losses due to piracy reported by the movie industry, the $2.3 million this project is estimated to cost seems like a good investment if it has any reasonable chance of success.

[9] There is some precedent in the music industry for trusted devices. It has been reported that recent CDs have been delivered to critics in sealed CD players (Nelson, 2002). These are considered *trusted players* because they must be returned unopened. Furthermore, a special player is required to play the DVDs released for airplane use.

[10] We will not, for now, consider devices that include their own physical output device (screen). Their introduction may reduce the risk of leakage, but significantly increase their size, power consumption, and cost.

[11] For brevity, we omit many details of the design and construction of the player hardware and software.

[12] Despite the difficulty of this task, the recording industry announced in June 2003 that it had begun searching file-sharing networks to find users who are sharing “substantial” numbers of music files (Associated Press, 2003). The RIAA filed hundreds of lawsuits against these users by the end of 2003 (Haberman, 2003b).

References

Associated Press. (2000, 17 November). First movie distributed via satellite opens in New York. *CNN.com*. (http://www.cnn.com/2000/TECH/computing/11/17/digital.theater.%ap/)

Associated Press. (2003, 26 June). Record industry to sue downloaders. *CNN.com*. (http://www.cnn.com/2003/TECH/internet/06/25/download.suits.ap/index.html)

Biddle, P., England, P., Peinado, M., & Willman, B. (2002, 18 November). The darknet and the future of content distribution. In *Proceedings of the 2002 acm workshop on digital rights management.* Washington, DC. (http://crypto.stanford.edu/DRM2002/darknet5.doc)

Butler, R. W. (2003, 22 June). Movie industry battles film piracy on many fronts. *The Kansas City Star*. (http://www.kansascity.com/mld/kansascitystar/6141893.htm)

Cheswick, W., Bellovin, S., & Rubin, A. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (Second ed.). ACM Books / Addison-Wesley.

Cinea. (2003a, 18 July). *Cinea demonstrates field ready security solution for major studios.* (http://www.cinea.com/press/press_release_new.htm)

Cinea. (2003b, 4 March). *Cinea, Sarnoff collaborate in developing anti-piracy technology to fight camcorder taping of movies in digital cinemas.* (http://www.cinea.com/press/press_release_03042003_2.htm)

Computer Emergency Response Team (CERT). (2004). *CERT Homepage.* (http://www.cert.org/)

Corperation, M. (2003, July). *Next Generation Secure Computing Base.* (http://www.microsoft.com/ngscb)

Cox, I., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *6*(12), 1673–1687.

Deloitte and Touche. (2003, June). *The impact of piracy on the film industry.*

Eller, C., & Cieply, M. (2003, 31 March). The movie watchers are being watched. *The Baltimore Sun*. (http://www.zeropaid.com/news/articles/auto/13302003c)

Garfinkel, S., & Spafford, G. (1996). *Practical UNIX and Internet Security* (Second ed.). O'Reilly.

Graham, T. (2003, 27 September). N.J. man, 24, is sentenced for Net bootleg of 'The Hulk'. *The Philadelphia Inquirer*. (http://www.philly.com/mld/inquirer/news/local/6873888.htm)

Gunter, C., Weeks, S., & Wright, A. (2001, January). Models and languages for digital rights. In *Proceedings of 34th annual hawaii int. conf. on system sciences (hicss).*

Haberman, L. (2003a, 10 June). Hulk: It's not easy being CG. *E! Online*. (http://story.news.yahoo.com/news?tmpl=story&cid=794&ncid=799&%e=1&u=/eo/20030610/en_movies_eo/11951)

Haberman, L. (2003b, 29 September). "Hulk" pirate walks plank. *E! Online*. (http://www.eonline.com/News/Items/0,1,12592,00.html)

Haller, N. (1994, February). The S/Key^{tm} One-Time Password System. In *Proceedings of 1994 internet society symposium on network and distributed system security* (p. 151-157). (San Diego, CA)

Huffstutter, P. (2003, 26 June). How Hulk crushed the online pirate. *Los Angeles Times*. (`http://www.latimes.com/business/la-fi-hulk26jun26224419,1,1391001.story`)

Mathews, A. W., Orwall, B., & Chen, K. (2003, 3 March). Pursuing Oscars, big studios give pirates a hand. *The Wall Street Journal*, A1.

McCarthy, E. (2002, 14 October). A new focus on movie piracy: Battling bootleggers with distortion. *The Washington Post*, E5. (`http://www.washingtonpost.com/c2/wp-dyn?pagename=article&node=&contentId=A18443-2002Oct12`)

McClam, E. (2003, 25 June). N.J. man pleads guilty to posting 'Hulk' bootleg. *Newsday.com*. (`http://www.newsday.com/news/local/wire/ny-bc-nj--hulkbootleg0%625jun25,0,5965106.story?coll=ny-ap-regional-wire`)

McDaniel, P. (2002). Authentication. In *The Internet Encyclopedia.* John Wiley and Sons, Inc.

Motion Picture Association of America. (2003). *Anti-piracy.* (`http://www.mpaa.org/anti-piracy/`)

Nelson, C. (2002, 16 September). Epic records takes steps to seal its newest music. *The New York Times*, C7.

Neumann, P. G. (1995). *Computer Related Risks* (First ed.). ACM Books / Addison-Wesley.

Ramanujapuram, A., & Ram, P. (1998, May). Digital content and intellectual property rights. *Dr. Dobb's Journal*.

Rea, S. (2003, 15 May). Studios battling movie piracy. *The Philadelphia Inquirer*. (`http://www.philly.com/mld/inquirer/news/frong/5864665.htm`)

Reuters. (2003, 26 June). N.J. man admits guilt over 'Hulk' bootleg. *CNN.com*.

Samuelson, P. (2003). DRM {and, or, vs.} the law. *Communications of the ACM*, *46*(4), 41–45.

Seiler, A., & Snider, M. (2003, 6 May). The movie industry fights off the pirates. *USA Today*. (`http://www.usatoday.com/tech/news/2003-05-06-movies-piracy_x.%htm`)

Serafini, D. (2003, March–April). DVD piracy in the U.S. becomes an industry. *Video Age International*, *23*(2). (`http://www.videoageinternational.com/2003/articles/March/pira%cy.htm`)

Taub, E. A. (2003, 19 June). Among film's ghosts, its future. *The New York Times*. (`http://www.nytimes.com/2003/06/19/technology/circuits/19cine.%html`)

Valenti, J. (2002, 23 April). *A clear present and future danger: The potential undoing of America's greatest export trade prize.* Testimony before the House Appropriations Subcommittee on Commerce, Justice, State, the Judiciary, and Related Agencies. (`http://www.mpaa.org/jack/2002/2002_04_23b.htm`)

Wray, R. (2003, 4 June). Matrix downloaded: Net piracy could cost film business billions. *The Guardian*. (`http://film.guardian.co.uk/news/story/0,12589,969754,00.html`)

	Number of Samples	Theater Internet Lag (days)	DVD Internet Lag (days)
Aggregate Sample Data			
Reviewed Samples	285	100	-83
Insider	220 (77%)	105	-79
Outsider	65 (23%)	86	-96
Sample Features			
Incomplete video editing†	4 (1%)	38	-192
Incomplete audio editing†	1 (<1%)	12	-362
Watermark or text marker†	35 (12%)	52	-141
VHS quality	6 (2%)	60	-149
DVD quality	223 (78%)	123	-62
Through-the-air video	46 (16%)	9	-171
Through-the-air audio⋆	39 (14%)	10	-171

Table 1: Classification of movies in sample. Numbers in parentheses represent percentage of reviewed samples. Features marked with a † represent conclusive evidence by themselves of insider leakage, and those marked with an ⋆ provide conclusive evidence of outsider leakage. Features without markings required additional information to classify as insider or outsider (e.g., release dates).

Studio	Releases in Data Set	Number of Releases Indexed on Content Verification Site	Number of Releases on DVD	Box Office Take Per Release (millions of $s)	Theater Internet Lag (days)	DVD Internet Lag (days)
20th Century Fox	25	15 (60%)	20	$64	96	-115
Buena Vista Pictures	17	10 (59%)	15	$79	132	-59
Columbia Pictures	27	19 (70%)	23	$58	66	-105
Dimension Films	7	5 (71%)	7	$20	146	-21
DreamWorks	9	5 (45%)	9	$71	100	-51
Fox Searchlight Pictures	8	6 (75%)	7	$19	42	-139
Lions Gate Films	9	5 (45%)	7	$9	77	-164
MGM/UA	19	12 (63%)	15	$25	77	-88
Miramax Films	23	9 (39%)	21	$21	108	-98
New Line Cinema	15	11 (73%)	12	$87	55	-130
Paramount Pictures	24	16 (67%)	21	$48	67	-86
Sony Pictures Classics	7	0 (0%)	6	$3	NA	NA
Touchstone Pictures	12	7 (58%)	12	$62	104	-55
Universal Pictures	18	15 (83%)	14	$76	69	-97
Warner Bros.	37	29 (78%)	30	$57	63	-103

Table 2: Statistics for each studio with five or more movies in our data set. All statistics include only the movies from each studio that are included in our data set. Box office take per release was calculated from data obtained from Rottentomatoes.com in July 2003. It represents the average box office take for the movies in our data set.

Figure 1: A preliminary version of the film “The Hulk” was criticized for the poor quality of its CGI. The watermarks in the bottom right corner were removed in an attempt to mask its origin.

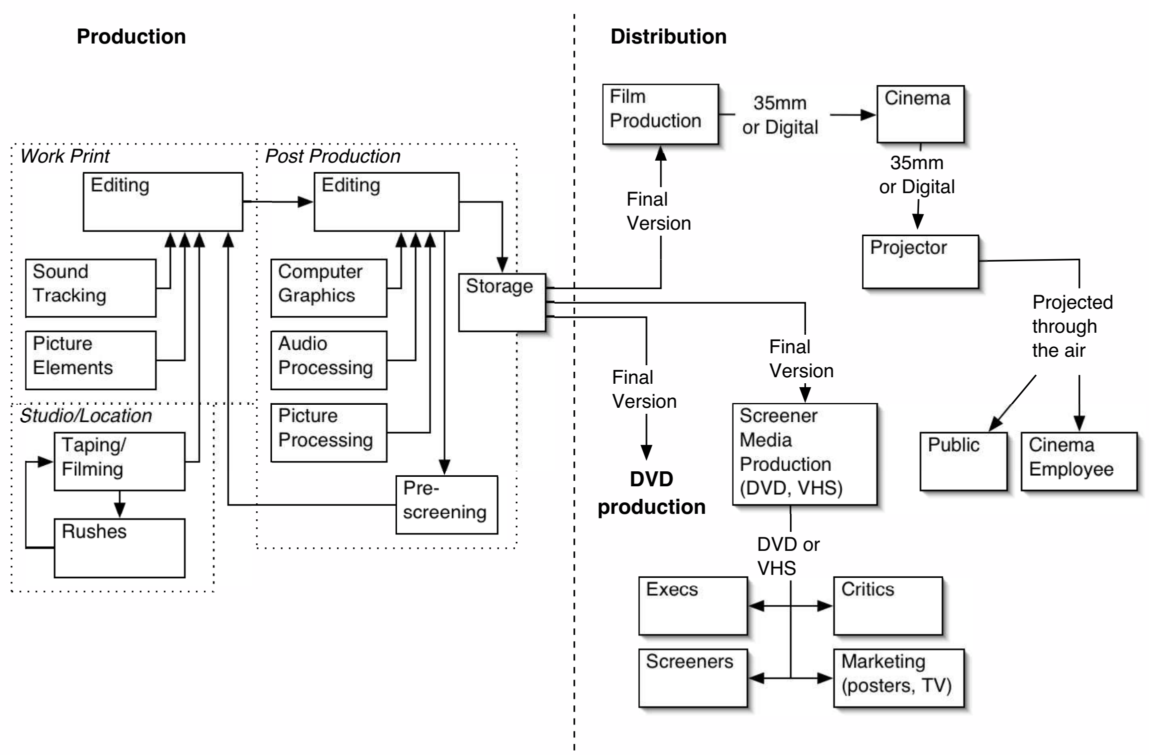

Figure 2: Movie production and distribution workflow. Content is cooperatively generated during the production process. The final product is replicated and delivered to the consumer during the distribution process.

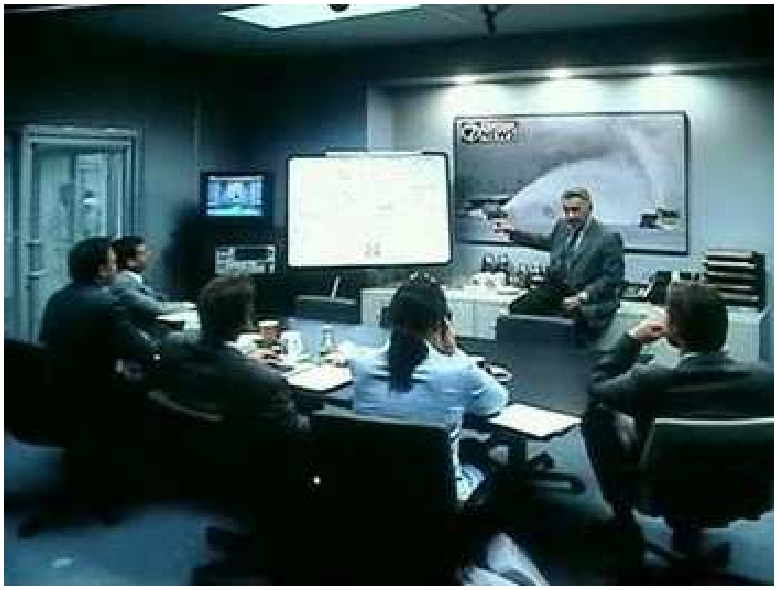

Figure 3: Editing room artifact – boom microphone in top center of film.

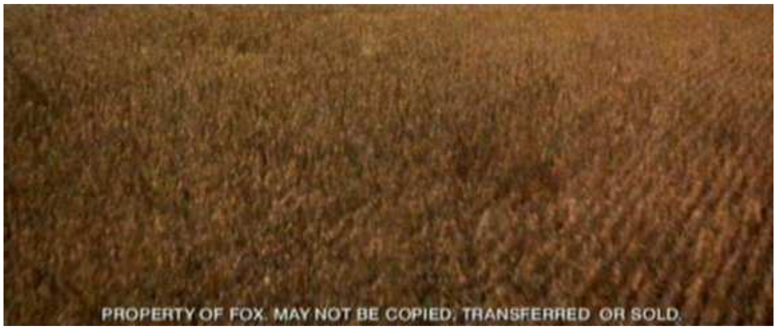

Figure 4: Studio "property" marking.

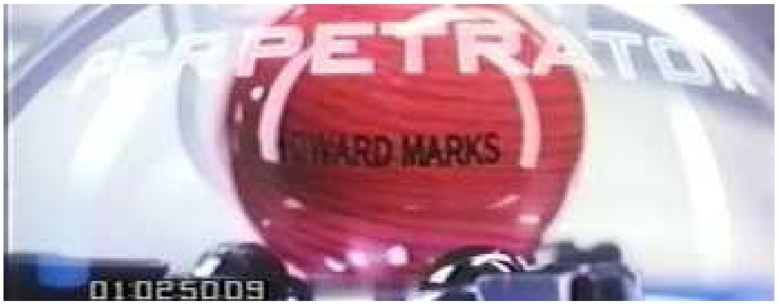

Figure 5: Production copy — note time code on bottom left and two blurred watermarks at bottom center.

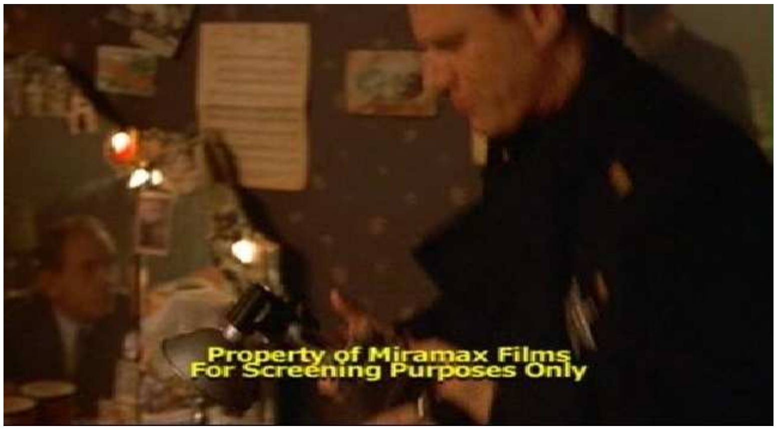

Figure 6: Screener text.

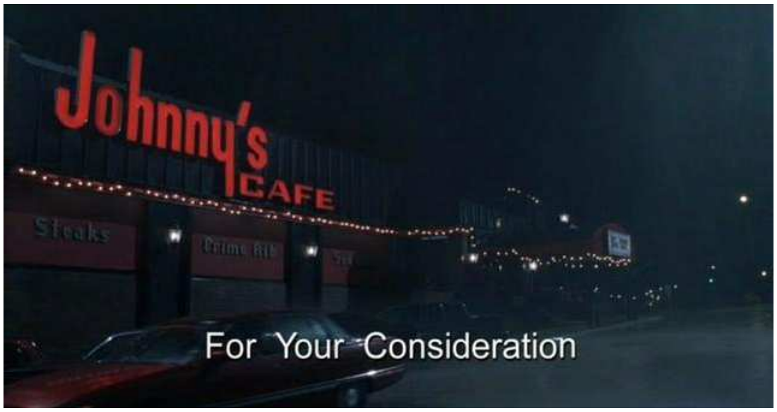

Figure 7: Copy marked as being for awards consideration.

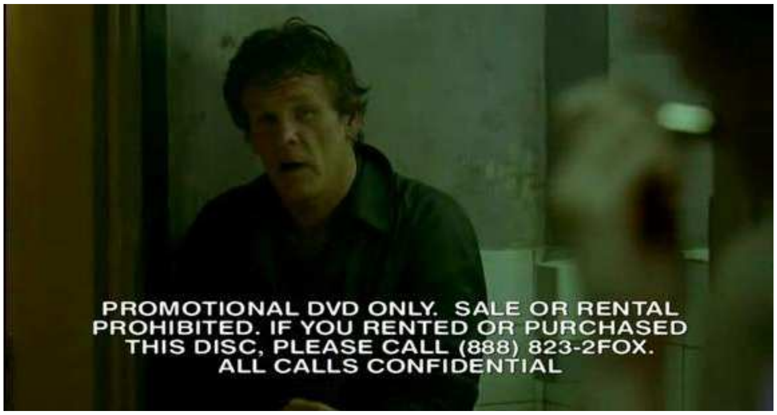
PROMOTIONAL DVD ONLY. SALE OR RENTAL PROHIBITED. IF YOU RENTED OR PURCHASED THIS DISC, PLEASE CALL (888) 823-2FOX. ALL CALLS CONFIDENTIAL

Figure 8: Copy marked as being a promotional DVD with explicit instructions for reporting leak.

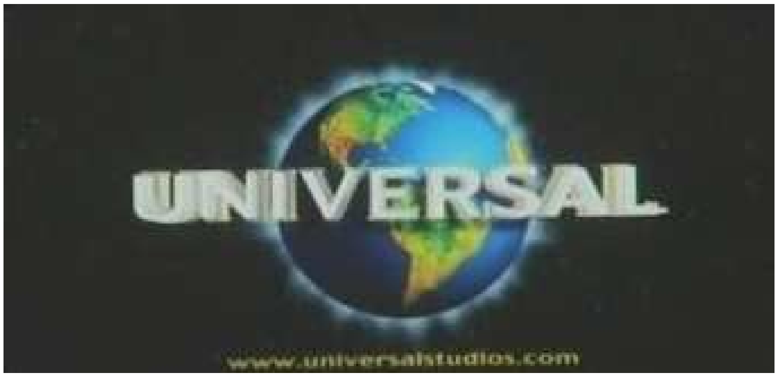

Figure 9: A frame from an unauthorized copy of a movie probably recoded through-the-air using a camcorder from a cinema seat. Note the slightly angled studio URL.

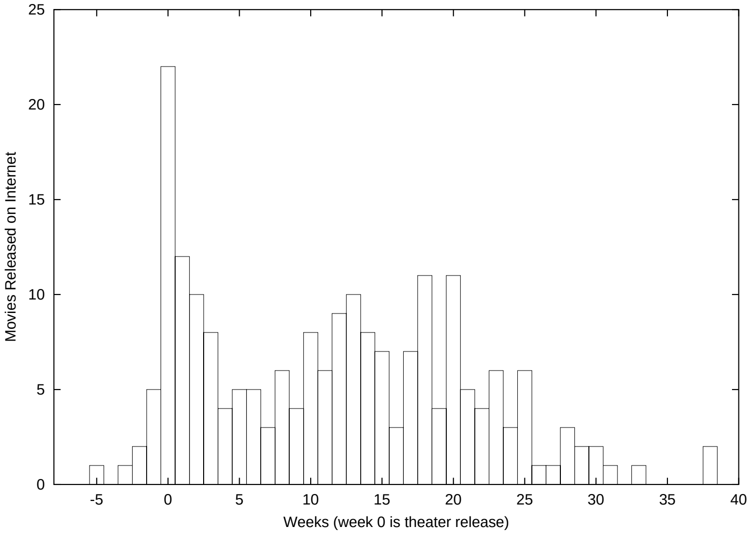

Figure 10: Distribution of theater/Internet release time lags for samples in our dataset. Week 0 is the week a movie was first released in U.S. theaters.

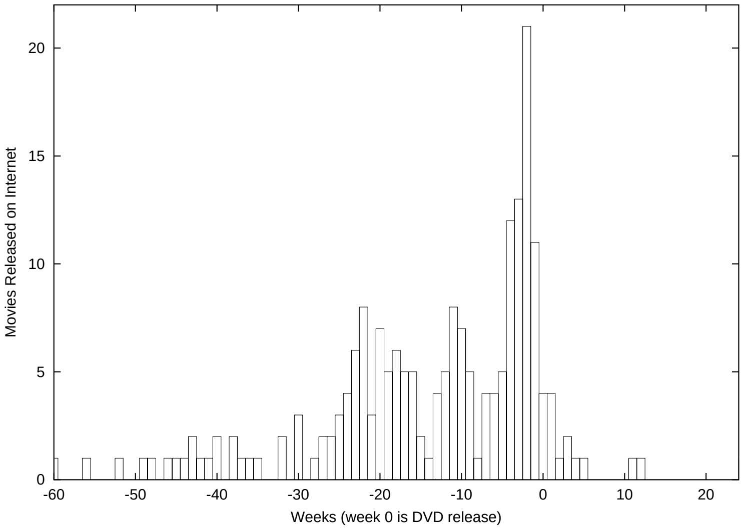

Figure 11: Distribution of DVD/Internet release time lags for samples in our data set. Week 0 is the week a movie was released officially to U.S. consumers on DVD.