



# **The DivX Networks Solution for Secure Internet Video: An Overview**

**November 15, 2001**

By Eric Grab  
Director of Engineering  
DivX Networks, Inc.  
10350 Science Center Drive  
Building 14, Suite 140  
San Diego, CA 92121  
[egrab@divxnetworks.com](mailto:egrab@divxnetworks.com)

## Company Overview

DivXNetworks, Inc. is a technology company that provides a complete solution for the secure and efficient delivery of full-screen, full-motion, DVD-quality video over Internet Protocol (IP) networks. Popularized by tens of millions of users worldwide, DivX™ is the emerging standard for broadband digital video and is the leading video compressor/decompressor (codec) based on the MPEG-4 international standard. With a significant technology lead over competing video compression technologies, DivX is becoming the standard for DVD-quality video over Internet Protocol networks, much like MP3 is the *de facto* standard for CD-quality Internet audio. DivXNetworks has leveraged the widespread adoption of DivX™ technology to create the DivX Open Video System, a secure, profitable video-on-demand (VOD) solution for IP networks.

## Introduction

DivXNetworks Inc. has developed a video-on-demand system optimized for the public Internet. This paper frames the problems associated with distributing video on the public Internet and describes DivXNetworks' reasonable solution to the problem.

Digital distribution of media files through the public Internet presents myriad legal, technological, sociological, economic, and moral implications. The digital music debacle begs the question: Is there a workable security solution tailored to the digital distribution paradigm? The Digital Millennium Copyright Act (DMCA) has done little to promote a sensible and practical examination of the issue of digital rights management (DRM). In the post-Napster era, all major Hollywood studios are moving toward an Internet Protocol (IP) based video-on-demand solution and hundreds of thousands of unprotected full-length films are transferred over the Internet daily [1]. The urgent need for a reasonable and workable approach to digital video security is underscored at every turn. An intelligent approach to digital rights management on the Internet should address business and technological issues through a software-based, flexible, rapid-response security solution.

## Video on the Internet

The rapidly converging digital media landscape has proven that content will be distributed over the Internet. The only real question for content owners, providers and aggregators is who will be doing the distribution. The complete elimination of piracy is an impossible goal; rather, the proper aim of secure Internet video is to help content providers ensure that **they** are the ones distributing (and thereby profiting from) their own content. To this end, digital rights management of video on the Internet must take a flexible, comprehensive, rapid-response approach designed to address security as a business, as well as a technological, issue.

## Two Big Risks

In the worst-case scenario of digital piracy, a piece of content is both widely distributed and unprotected. This can result from two different phenomena:

1. Mass distribution of unprotected content via underground channels
2. Mass "cracking" or non-protection of legitimately distributed protected content

The first case represents the well-known Napster effect: wholly unprotected digital CD audio were compressed and massively distributed by the Napster client. The second scenario can be seen through DeCSS and related technologies that have “broken” DVD security, opening the door to the widespread and relatively simple breaking of protection on legitimately distributed content.

The key word in the two scenarios above is **not** “unprotected”; it is “mass”. The unique and tremendous risk of Internet distribution is that computers and digital networks enable a rapid and massive scale unknown to any other form of piracy.

### **Scaling Piracy: The Conundrum of Digital Distribution**

With over 50 years of refinement, the computer has perfected the science of moving and copying digital data. This is an essential function of the platform. One cannot, or should not, expect to modify this fundamental nature. Consequently, once a piece of content is in a digital format, it is out of the control of the content owner in a way that few other distribution methods demand. Given this fact, why should video content providers run the risk of lost revenue and lost control? Why not abandon digital distribution or even digitization entirely? Frankly, because this is not a viable option for content owners who wish to continue to succeed in the digital era.

### **Big Picture: From Reality to Reality Reproduction**

The diagram “From Reality to Reality Reproduction” shows the flow from reality to reproduced reality. It portrays analog, digital, protected, and unprotected distribution. Images and sound flow through capture devices, several formats, and are eventually rendered for eyes and ears. A large body of technology and techniques span this flow. It is important to note that each stage in this path is vulnerable to unauthorized copying, digitization and distribution. Restricting content to traditional physical distribution media, like DVD or CD, is ineffective. And locking content exclusively in the analog domain is similarly problematic – digitization is easy and one analog-digital conversion can be made with little degradation of quality. Indeed, taking the step of prohibiting all distribution will still not solve the problem. For example, a master tape duplicated during post-production can be digitized and made available for digital distribution in Asia on one day, pirated the next and globally distributed free of charge by the end of the week.

The diagram below illustrates, multiple opportunities for breaks throughout the content production and distribution process. It only takes one “break” to compromise security on a global scale.

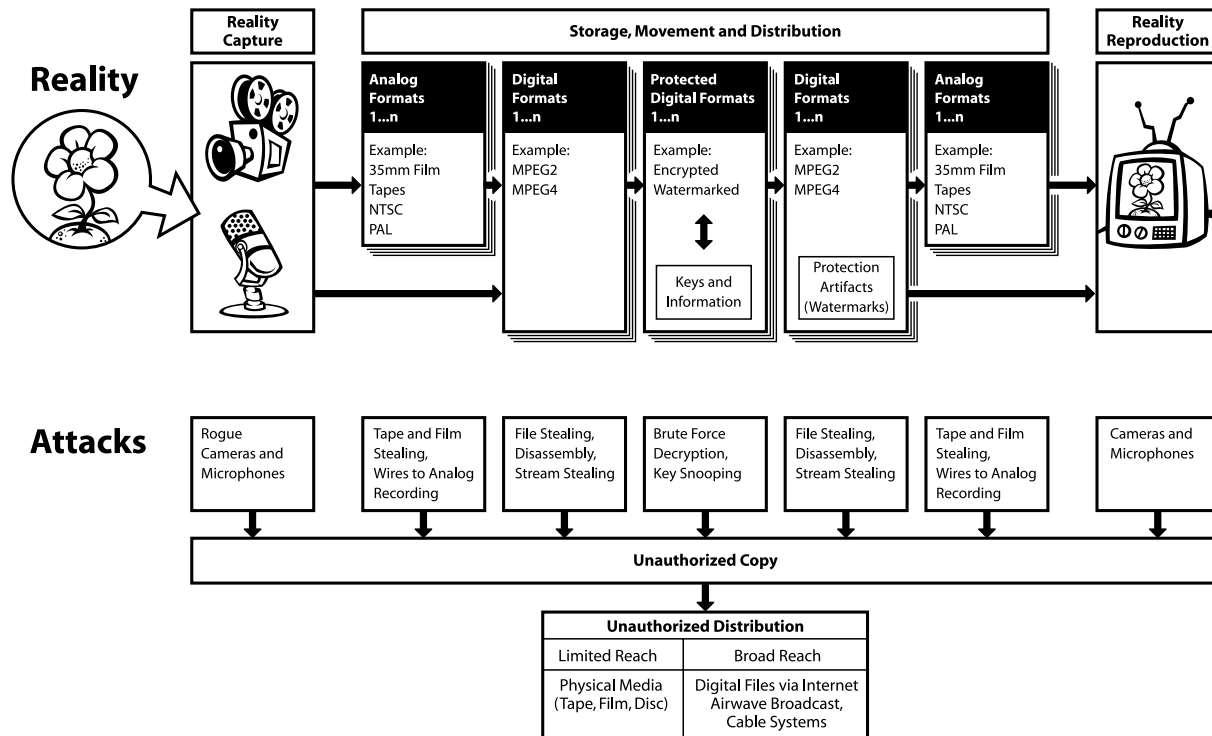


Diagram 1. - From Reality to Reality

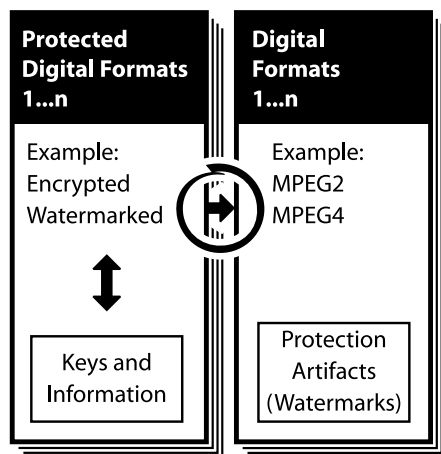
Clearly, as long as human beings are interested in creating content in some medium outside of their own heads, that content is vulnerable to rapid and massive digital piracy. Imagining the scope of the problem can churn even the strongest stomachs. However, if one analyzes the problem carefully and takes a reasonable approach, it is possible to successfully navigate the digital distribution minefield.

### Focusing on the Threat

Given that there is no easy way to avoid being affected by digital piracy, what is the best method to effectively solve the problem? Remember the two most plausible digital piracy scenarios:

1. Mass distribution of unprotected content via underground channels; and
2. Mass “cracking” or non-protection of legitimately distributed protected content

These scenarios correspond to the sections highlighted in the diagram below:



Unauthorized Distribution	
Limited Reach	Broad Reach
Physical Media (Tape, Film, Disc)	Digital Files via Internet Airwave Broadcast, Cable Systems

Diagram 2. – Threat Focus Areas

Addressing the first problem of mass distribution requires a potent mix of litigation, legislation and business initiatives outside the scope of this paper. It is worth suggesting, however, that the only truly effective solution to mass distribution via underground channels is to provide better, easier-to-use legitimate channels that both marginalize and displace the underground. It is important to note that any effort to do this imposes very specific requirements on digital rights management solutions: they cannot be so burdensome to the end user that they make legitimate content harder to get and use than pirate content.

The immediate focus of DRM, then, is the second problem: the mass non-protection of legitimately distributed content. Again, the core problem is not merely “non-protection”; it is “mass unprotection”. There will always be someone who can break any form of protection with sufficient time and expertise. A significant threat is not posed by a handful of rogue hackers with PhD’s in both information theory and hardware design--unless they effectively artifact their expertise into a simple program or device that makes cracking content a trivial (and, therefore, mass) endeavor. This kind of phenomenon is labeled a “black box.”

In the analog world, a black box refers to a pirated device that unscrambles cable channels and allows consumers to access the system for free. In the world of Internet digital video, an example of a black box is the by now infamous DeCSS code, which is a cracking scheme that enables the mass break of DVD encryption code. The existence of DeCSS enabled the breaking and ripping

of DVDs to move from the margins to the mass. Thus, the black box phenomenon is the primary threat to the legal and protected distribution of mainstream video content on the Internet today.

The Digital Millennium Copyright Act (DMCA) outlawed black boxes, and various legal cases involving DeCSS have been followed extensively in the digital video community. The spirit and letter of the DMCA state explicitly that if protection is applied to a copyrighted file and that protection is broken, the offending party has broken the law. This is an interesting development for digital rights management in that it gives legal power to content publishers to prosecute when security has been violated, as long as they can identify the offenders.

## Reacting to the Threat

There are two strategies to counter the immediate threat of mass non-protection:

1. **Defeat black boxes** – As demonstrated by DeCSS, the biggest threat to the protected distribution of digital video is the black box phenomenon. The ideal security approach will defeat black boxes by preventing the break of one piece of content from breaking all subsequent content.
2. **Ensure Prosecution** – Because the DMCA identifies clear legal consequences for the violation of digital copyright, the ideal DRM solution will provide traceability to ensure that offenders can be prosecuted. For the principles established by the DMCA to hold any practical significance in the real world, it must be possible for content owners to track down copyright violators and fine or sue them. Current fines for first-time violators are around \$2500, and go up to \$1 million for repeat offenders who have defeated encryption [2]

This is a forward-looking strategy for video security, as it is difficult to defeat black boxes and start litigation for current digital content. DVDs, for instance, cannot change current encryption because of the installed hardware base and standards. A more interesting case can be seen with audio compact discs, where any attempt to protect the format in the short-term would effectively break all the devices on the market without ever identifying the offender. Indeed a new set of devices and software must be in place to make this work, and how to reasonably organize such a solution is the next logical question.

## Security Techniques and Concepts

To formulate a reasonable approach, it is necessary to first examine the different techniques that can be applied to digital video on the Internet. Following is an attempt to categorize various approaches to security:

- **Encryption** –Encryption adds a lock around the content.
- **Decryption** –Decryption unlocks the content for playback. With video content, decryption must move very quickly.
- **Key Management and Authentication** – Key Management addresses movement of the keys that allow a user to decrypt content. Keys should only be used by components that are authenticated and trusted.

- **Business Rule(s)** – Encryption/decryption need context to operate. Business Rules or licensing information determines when to unlock the content so it can be viewed. The business rules couple two parties, such as the distributor and the viewer via a transaction.
- **Watermarking** – Watermarking adds information to the content, and can use techniques similar to encryption. It can be either visible or invisible, and is usually woven in the content such that removing the mark will degrade the video to some degree. The information embedded can include the source and owner of the content and/or information regarding who is allowed to access it. When watermarking traces back to a single party or user, it is commonly called fingerprinting.
- **Watermark Reading** - Similar to decryption, Watermark Reading displays information imprinted with a watermark.
- **Tamper Resistance** – Tamper Resistance is meta-security, designed to ensure that business rules and decryption are not short-circuited. Also known as “hardening”. Typically very difficult, if not impossible to do in software, because hardware can always be used to snoop the workings of the software.
- **Renewability** – Renewability refers to the technique of modifying or de-authenticating aspects of the system as appropriate. Obviously, it is critical to update any kind of security.
- **Geographic Location** – Given an IP address, the geographic location can be derived. In the case of country it is 99% certainty. This can be used in geographic region enforcement.

There is one invariant to video content protection. Video will **always** become unprotected at some point simply because a user’s eyes and ears must be able to access it. All forms of protection have this obstacle as a weakness. As long as the technology to record and copy content is inexpensive to the masses, complete protection is impossible. When data writing technology is magnitudes more expensive than data reading technology there is a false sense of protection. For a window of time a 650 megabyte compact disc was well over 10 times the space of most writable storage devices, and the processing power for compression was seemingly ages away. At present, writing a CD is trivial, and compression of data is common. However it is important to note that visible or invisible information such as watermarks can persist across copies.

Clearly, there is no single “silver bullet” approach to securing anything, as all the pieces described above are designed to work together to be effective. The key to designing the reasonable solution is how, when and where these various components are combined to reach the most desirable result.

### **A Reasonable Technology Approach**

A security system is only as good as it’s weakest link. It is important to combine the available tools and techniques to make an overall secure system. The principle of easiest penetration applies [3]:

An intruder must be expected to use any available means of penetration. This will not necessarily be the most obvious means, nor will it necessarily be the one against which the most solid defense has been installed.

So given our point in time and technology, what does the feasible system look like? Most importantly, the solution must address black boxes and facilitate DCMA litigation. Given such a premise, a client server software system with security at various points makes the most sense. This is the DivXNetworks Open Video System (OVS). It includes the following:

- **Rapid Response Software Based and Updates** – With the proper level of video compression and processing power, software can run entire video systems while ensuring content protection. The assertion is that only software can be created and updated quickly enough to address black box attacks. Software is easier to change and deploy than hardware. If any piece of the security solution becomes broken, the software solution allows it to be fixed dynamically. This methodology includes changing an interface, or adding more tamper resistance.
- **Software Tamper Resistance** – Software executables can be disassembled with tools, requiring technologies and techniques that remove debugging information and scramble the binary code that makes it difficult for readily available tools to disassemble.
- **Encrypted Content** – Video content is encrypted and is never stored on a system in an unencrypted form. Additionally, consumers naturally expect “trick play” (fast forward, rewind, pause), so the encryption scheme incorporates this functionality.
- **Communication Channels Encrypted** – Certain elements of the system will exist over plain communication channels. The components communicate securely in order to prevent packet sniffers.
- **Content Watermarking** – Core to protecting content is the ability to trace content. The watermark includes identity of the content owner and date. This provides an immediate handle on what further forensic tools can be used to trace the content.
- **Transaction Watermarking** – The second form of watermarking, transaction watermarking is similar to content watermarking except that each copy of the content contains targeted information on the intended recipient. This form of watermarking makes it possible to pursue DMCA litigation by proving that unauthorized individuals have accessed content. In this process, content is actually decrypted, marked, and then encrypted. Transaction watermarking is made possible only with an exceedingly efficient encryption solution in place.
- **Server Side Business Rule(s) and Key Management** – The only software that can be completely trusted is software under the distributor’s control. A central service holds the decryption keys and makes the conditional access decisions. Keys are only held at the client long enough to decrypt, and never stored locally, which helps with tamper resistance as well. Additionally, business rules can be easily changed to meet the needs of the consumer and content provider.
- **Geographic Region Enforcement** – Distributions rights can define where it is legal to distribute and use content. The ability to detect where a consumer is actually using the content makes region enforcement possible. If the user is not in the correct area, the content cannot be purchased.

- **Server File Access Protection and Recovery**—The content files need to be stored on a server. You can only download a file if you have paid. This happens with a temporary username and password to access the file download. Also you can only download the file once. The server remembers what percentage of the file was downloaded. This also allows intelligent recovery of partial downloads.

## Example Interaction

In order to make the above approach a bit more concrete here is an informal dialog of how a the client and server interact:

### Success Scenario 1 – Get A Movie

Client: Hello, I am version 1.0, is that ok? (if not ok, need to get update)

Server: Yes, 1.0 is ok.

Client: My user's name is Alice, the user's password is Secret.

Server: I recognize that user, how can I help you?

Client: Please get me movie title.

Server: Ok, it costs \$1.95 for two day rental, please send me some money.

Client: Here is the money (credit card, or micro payment information sent).

Server: Ok, got the money. Here is your transaction id.

Client: I got the id, please send me the movie.

Server: Here is chunk 1 of the movie.

Client: I need to unlock the movie. I need the key.

Server: Your rental is still valid, Here is the key.

Client: I fingerprinted the movie 1 chunk with the transaction id and saved it.

Server: I recorded you got chunk 1. Here is the next chunk.

Client: I am decrypting a chunk and sending to the display.

Of course the DivXNetworks OVS has many more and detailed interactions.

## More Than Technology: The Complete Perspective

It is important to consider that technology is not the only issue crucial to effective video distribution on the Internet. The truly complete security solution for Internet video also considers, business, psychological and legal aspects of the problem. In fact using all of these aspects together is what can make video on the Internet happen. Here we are in 2001 and looking at these:

- **Psychology**—It is crucial that the right approach take into account the mind set of the end user and the potential copyright violator. Utilizing a rapid response approach and fingerprinting technology makes it difficult for the potential violator. Perhaps most importantly, the ideal solution must make purchasing legal, protected video content easier and more attractive to the consumer than downloading pirated content.
- **Legal**—Watermarking and fingerprinting technologies ensure maximum traceability in the event that security is compromised, allowing content owners to litigate. Organizations need to have the dedication and resources in place to follow through. This includes actively monitoring and detecting violations.

- Business**— There are several business considerations, including what to charge, and how to charge for it. Right now consumers understand purchases and rentals. It is entirely possible to investigate other methods of payment and advertising revenue. But marketing and business interests need to ensure consumers are trained in these new models. The overall solution needs to be flexible enough to meet needs of the consumer and the content provider alike. Also, the content owners have to understand the models and value of video on the Internet to make business decisions.

Putting it all together, we get the complete perspective illustrated in diagram 3.

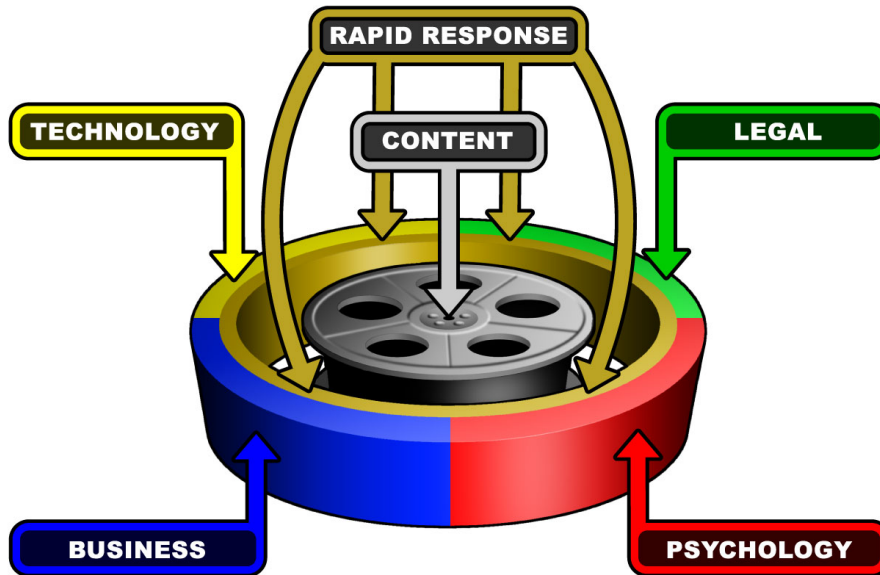


Diagram 3 – The Complete Perspective

## Conclusion

Daunting challenges face all parties involved in the digital distribution of video over the Internet. The first step to developing a reasonable security solution lies in identifying and fully understanding these challenges. Unprotected video files are being distributed online at a growing rate, and the recent video-on-demand announcements from major Hollywood studios demonstrate that secure content is a necessary business condition for mainstream digital distribution to become a reality. Given the current threat, the most reasonable and comprehensive approach to digital rights management is a software-based, rapid response solution designed to address the technological, business, legal and psychological components of digital piracy. This solution is the Open Video System by DivXNetworks, Inc.

## REFERENCES

[1] Vidius - "We're tracking 450,000 to 580,000 downloads a day on average," said Derek Broes, chief executive of Vidius Inc, April 2001, Associated Press

[2] Digital Millennium Copyright Act (DCMA), October 1998, Public Law 105-304.

[3] Pfleeger, "Security in Computing", 1989 Prentice Hall ISBN 0-13-798943-1



For More Information, contact:

Eric Grab

Director of Engineering

DivXNetworks, Inc.

858-909-5311

[egrab@divxnetworks.com](mailto:egrab@divxnetworks.com)