SECURITY AND STREAMING MEDIA – HOW TO SECURE YOUR VIDEO AND PROTECT YOUR REVENUE

Mark D. Fears
Director, New Product Development
ViewCast Corporation, USA

ABSTRACT

As more and more popular applications come on the market such as streaming video to cell phones, video blogging and streaming inside the networked home, security is key to protecting content and privacy. There are multiple ways to secure and protect your streaming media so that confidential or sensitive content doesn’t end up in the wrong hands or distributed to an unauthorized audience. In this session we’ll talk about ways to protect content with software, DRM and new techniques in video streaming like dynamic watermarking.

Security vulnerabilities are concerns that should be addressed because in many cases there are lost revenues and ownership rights at stake. Come learn about the vulnerabilities and the ways you can protect your system against intrusion and content against piracy.

INTRODUCTION

As video distribution explodes so does the risk of piracy and the need for securing content from unauthorized access and piracy. While the debate rages on the effectiveness (and fairness) of Digital Rights Management (DRM) versus consumer rights, this encryption and keying method is only one of many tools the content creator can instigate to inhibit unauthorized viewing. Other methods for protecting content that are not as invasive can be deployed and, for certain applications, can actually be more effective.

This paper examines ways to protect streaming video content using different techniques and technologies. Security-enabled networks, Digital Rights Management (DRM) encryption and dynamic watermarking are the most popular methods that this document will review and diagram the infrastructure or method. Although all of these can be implemented in unison, one or two will be adequate to protect your content. It is important to understand that each represent a different level of security and with higher security comes more restricted distribution. In some applications, unrestricted distribution could be more important than security.

CHOOSING THE SECURITY LEVEL

Different applications require different levels of security measures to be implemented. Using the security methods mentioned in the previous section, let’s try to define a scale and rank each method on that scale.
Restricting the access to the content by placing on a secure private network would rank as a high-
level security measure. After all, the best way to secure your content is not to distribute it publicly. 
At the opposite end of the spectrum, watermarking the video with a brand would rank as a low-level 
measure. The most important aspect to understand is that the 
greater security method you deploy, the more restricted the 
distribution of the content. So you must weight the importance of 
broad distribution against the importance of protecting the content.

For example, if I created a product sales demonstration video, I 
would want access of that content to a broad audience of potential 
customers. I would choose the low-security measure to protect my 
content. The logic: broad distribution of the content is paramount while copy protection and 
restrictive access are not.

It is important that the content maintains corporate branding so that it couldn’t be edited and used by 
others for their own purposes. There is a significant expense to creating the content and if I have 
licensed third-party content in my video message, I have an obligation, typically detailed in a third-
party license agreement, to protect the ownership and distribution rights of the licensor.

A high-level security example is corporate content to be distributed to a small closed network of 
viewers.

In my role as Director, New Product Development, for ViewCast Corporation, I am required to 
create and maintain the product development strategy and roadmaps. I am also responsible for 
communicating these strategies to the executive staff and department managers, which typically 
takes the form of a presentation. For participants that can’t physically be present for travel reasons 
and also to document the presentation, the event can be captured on video. This content would 
require high-security measures that could use a couple of methods for protection. They would be 
closed distribution on a security-enabled network and content watermarking with corporate logo and 
confidentiality tag.

Since video communications has become commonplace in corporate environments, the ability to 
restrict access and limit distribution of corporate video content has become a great concern. Much 
like document encryption or password-protect networks, video content must be protected and secure 
to ensure that it distribution and access are tightly controlled.

In the last example, the focus is the restriction of access with extremely limited distribution. 
Security is increased while distribution is decreased.

As you increase your security measure, you limit the ability to 
distribute your content to a broad audience. In some 
applications, not only is this acceptable but absolutely 
intended. However in the first example, the content is intended 
for mass distribution and so a copy protection method, such as 
encryption, are exchanged for a low-level security measure 
such as watermarking or branding the content.

The greater the security method, the more restricted the 
distribution of content can be. These two factors act against 
each other and the deployment of these methods must find the right balance.
SECURE NETWORK METHOD

The easiest and most effective method of protecting your content is not to allow anyone to be able access it however the value of the content is negated if no one can view it. The first step is to restrict the ability for viewing to only those that you intend. This can easily be accomplished by placing the content on a streaming server that is located behind a firewall on a private network.

Just like a document server on a corporate network, your content will reside on a streaming media server that is located on a restricted network. The content is protected because only trusted viewers have access to the network on which the content resides. Even if the intended viewer resides outside the network, they can use the Microsoft Virtual Private Network (VPN) protocol to access the network and then view the content. This would require that the network include a VPN server.

Another method of restricted access, even on a private network, is to hide the IP address of the content. This is accomplished by simply providing the address only to those that you wish to view the content.

The streaming server itself provides additional security measures. Besides creating log files that include client IP address, time and date of content access, they provide content settings that can restrict the client’s ability to save the content making it a streaming view only. This prohibits the client from saving a file copy of the stream on their local hard drive and then distributing the file outside the corporate network.

ENCRIPTION AND KEY METHOD (DRM)

For users that need broad distribution of their content but want to restrict viewing, DRM has become the widely accepted method for securing their content to authorized viewing only. In this model, the content is posted on a streaming media server residing on the Internet while the link to view that content is then posted on a public web site. When a client clicks the link, they are required to perform an action such as provide personal information or purchase a license to view the content before the content is streamed to their PC.

The basic components that make up a DRM system are:

- Content that has been encrypted with DRM protection
- License key that decrypts the DRM protected content
- Third-party license provider

There are two ways that you can encrypt content with DRM protection. You can include the encryption when you capture the content into a streaming format or you can import a video file into your streaming media CODEC and create a new file with DRM protection.

In this process, the header of the resulting DRM protected file includes a web address for the license provider. It also includes the DRM encryption. This encryption requires a license key in order for the content to be viewed. The license key itself will be created when the content is encrypted.

The license key is then securely transmitted or delivered to the third-party license provider. The license provider will place these keys into their database to be delivered to the client upon request.
The encrypted content is placed on a streaming media server and the content access link is placed on a web page.

When the client clicks the web link to view the content, their streaming media player reads this header information and redirects the client to the license provider web page – the web address included in the content header. The license provider typically customizes this page to the content owner’s specification or corporate branding. On this web page, the client will be required to perform some task, such as a transaction.

Once the task has been completed the license provider will transmit the license key to the client’s streaming media player. The key will unlock the content and the client will be able to view the stream.

The license key is not transferable so that the client may not pass the ability to view the content to another person or copy that license to another PC.

The above method describes a DRM system for streaming media, however DRM can be used for other models such as copy protection or subscription viewing.

The third-party license provider can also limit the rights of the client based upon a criteria the content owner provides. For example, the license could have subscription rights. This would allow a client to purchase a license and be able to view that content multiple times with the license set to expire after a predetermined period of time has passed.

**BRANDING METHOD**

The last method, which is also the least restrictive for distribution and viewing when solely used, is branding the content. This branding can occur in a few different ways such as adding content ownership and copyright information in the stream header but the most effective method is watermarking the video.

Watermarking can simply be defined as the process of embedding data into another object or signal. High-quality papers have “hidden” watermarks that can only be viewed while backlit from a strong light source. Paper currencies include watermarks to make counterfeiting more difficult and easily detected.

Video watermarking is quite different from document watermarking since it is a series of images whereby each frame is imaged with a watermark. This watermark image resides in an area of the video that will not restrict the viewing of the content but brands each frame of video with a mark that represents ownership.

For example, Bill has created original content that he wants to distribute. He makes a copy of the original content adding a watermark to the copy. This copy is used for distribution while the original is kept secure. If Fred takes the copy and adds his watermark, then dispute of ownership can easily be resolved since Bill has the original content without the watermark and Fred’s includes both his and Bill’s signature watermarks.

When streaming video, adding a watermark is done during the encoding process. The source content is captured and a watermark is added during the encoding process. When the content is viewed the watermark is seen overlaying the video frames and can be made more or less apparent by setting the opacity of the watermark.
For a live event, the content can be captured with and without a watermark. This would require two encoding sessions making one captured file an original archive without a watermark and a watermarked version for streaming distribution.

CONCLUSION

In this paper, I have presented three methods for protecting streaming video content. Each method can be used independently or all three in unison to provide maximum protection.

It is important to understand that the more secure method of content protection deployed, the more restrictive the ability to broadly distribute the content will become. Each application objective must be examined and evaluated to ensure the appropriate security measures are used.

These approaches add a measure of security but are primarily intended to inhibit or reduce the threat of content piracy. As with any security model, a dedicated hacker over time can successfully circumvent these measures. I believe the methods presented will create a significant amount of work that will successfully deter most potential threats or isolate it to a particular piece of content.

©2006 All Rights Reserved ViewCast Corporation.