Protecting Online Video Distribution with Adobe Flash Media Technology

Table of contents

Introduction

Online video is a growing phenomenon. Record numbers of people are going online to watch everything from user-generated videos and breaking news events to television programs and full-length movies. Gone are the days of waiting for a program to air; consumers can now choose from a plethora of high-quality content, available on-demand.

From advertising-funded videos to subscriptions to pay-per-view, content providers are adapting a variety of business models to monetize content in the online world. As an owner or distributor of premium commercial content, such as films and TV shows, you must ensure that hackers do not bypass your business model or violate your copyrights.

Content protection solutions help create and preserve revenue streams; maintain copyright; and preserve content integrity or privacy. For instance, hackers may attempt to bypass payment in a pay-per-view model. Others may try to rip your content for redistribution. Worse, someone could try to make money from pirated content, or may introduce their own advertising or branding but skip paying content licenses or bandwidth fees by piggybacking on your distribution platform. In an enterprise situation, a disgruntled employee may be tempted to post valuable or private company information on public video sites.

Finding the right balance between user experience and content protection is critical. Adobe offers a number of solutions to help secure online video while creating an intuitive and engaging user experience.

This white paper presents Adobe Flash Media Server content protection features and best practices, and introduces Adobe Flash Media Rights Management Server.

Overview of Adobe video distribution solutions

The Adobe Flash Platform is the industry-leading solution for online video. The choice of many broadcasters, Content Distribution Networks (CDNs), and online retailers, Adobe Flash Media Server delivers live and on-demand content to millions of users a day around the world via the ubiquitous Flash Player. Worldwide, 98% of desktops have the Adobe Flash Player[1] installed. Approximately 80% of all online video—from short clips and live events to TV shows and

1. May 2009data from independent research firm comScore

Adobe

movies—is viewed using Flash Player . Flash Media Server 3.5 incorporates proven security features that allow you to support your business model while delivering high quality live or on-demand video.

While Flash Media Server offers suitable security for many types of streaming video solutions, some applications require more robust, persistent content protection and the ability to support business models such as download-to-own and offline video playback. Adobe Flash Media Rights Management Server, introduced in 2008, addresses these needs. This advanced digital rights management (DRM) solution lets content owners, distributors, and advertisers confidently deliver premium commercial content online using a variety of business models.

Best practices for effective content protection

A content protection solution for online video requires more than data encryption. Any solution must anticipate and proactively discourage circumvention attempts. In the event of a security breach, an effective response may include both technical and legal measures that can quickly restore an adequate level of protection.

On the technical side, the best solutions rely on robust cryptographic algorithms vetted by the security community. In addition, if a hacker compromises a client, the solution provider must block compromised clients from accessing protected content and quickly distribute an updated, secure version of the client. Just as importantly, the ideal solution should support an interactive and engaging user experience on a range of consumer platforms, while enabling content monetization through a variety of business models.

Flash Media Server content protection features

Flash Media Server incorporates proven security mechanisms that allow secure streaming to Microsoft® Windows®, Apple® Macintosh®, and Linux platforms, via Flash Player in the browser or a standalone application based on Adobe AIR. Flash Media Server also supports secure streaming to mobile devices via Flash Lite. Future digital home and consumer electronic devices will also support the same security techniques. Protecting video distribution with Flash Media Server is simple and seamless for both you and your customers. Flash Media Server has built-in security features that you can easily configure to start protecting distributed video. These security features are also part of Flash Player, Adobe AIR, and Flash Lite, so your customers do not need to download new software.

Flash Media Server also helps you easily and confidently monetize your video assets through a variety of business models. You can offer rentals, purchasing options, and subscriptions. You can also support video monetization through advertising, incorporating options such as overlays and pre- and in-roll advertisements.

The following security mechanisms help ensure your video reaches only the intended recipients with the desired user experience.

Real time protocol encryption

RTMPE (Real-Time Media Protocol Encrypted) is a secure streaming protocol that encrypts the stream between the server and the client. Because RTMPE was designed specifically to protect video content between Flash Media Server and supporting clients, it results in a better user experience and eases the management burden on the server. RTMPE uses 128-bit encryption to help prevent third-party applications or "network sniffers" from capturing the video from the stream. The client and Flash Media Server negotiate a session key between them, helping block "replay" attacks.

RTMPS (Real-Time Media Protocol over SSL) is Adobe's streaming protocol sent over a secure tunnel using industry-standard Secure Socket Layer (SSL). SSL secures TCP/IP connections and protects all data sent over the connection. CDNs do not typically use this level of encryption because SSL certificates are not easily deployed over a public CDN.

SWF verification

Developers create custom video players using Adobe Flash Professional or Adobe Flex. These video players are in a SWF (Shockwave Flash, pronounced "swiff") file format that runs in either Adobe Flash Player or Adobe AIR on the client's computer. SWF verification helps protect against "deep linking" or the theft of the video URL embedded within the SWF. Developers publish a SWF file at their web host to be downloaded within a web page, and place an identical copy on Flash Media Server. When a connection is requested, the Flash Player computes a cryptographic hash of the SWF and transmits the hash to the server. Flash Media Server compares this hash against the hash of the SWF it has stored and denies the connection if there is a mismatch. SWF verification prevents someone from creating alternative video players that can play your content without your video player. You should use this feature with RTMPE to ensure maximum protection. You can read more about these features here:

http://go.adobe.com/kb/ts_kb405456_en-us

Token-based authentication

To confirm publisher identity, many CDNs offer their customers a token-based authentication mechanism that ties content access to an authentication and authorization step completed at the web portal. Flash Media Server has an extensible plugin and scripting architecture that CDNs can use to integrate their own custom token-based authentication system with Flash Media Server. Before connecting to the CDN, the video player must obtain a token from the web portal. This token has a short validity period (or TTL, which stands for time-to-live) that provides protection against unauthorized replay. Token-based authentication helps you enforce your particular business model. For example, you can process an e-commerce transaction or check a user ID against a subscription database on your system, and then authorize content access on the CDN through a unique URL.

Domain limiting and geo-limiting

Flash Media Server can restrict access to specific domains or IP addresses (also known as the white list), or exclude certain domains or IP addresses (known as the black list). Using a geo-limiting plug-in for Flash Media Server, you can also abide by licensing agreements by limiting customers to markets you are licensed to serve. For example, a television network in a given country can allow only users located in that country to view their shows.

Integration with Directory Services

Through a plug-in, Flash Media Server allows you to integrate your video distribution with existing user authorization and billing systems and with existing access protocols, including LDAP and Active Directory.

The following example demonstrates how these security features can work together to secure valuable video assets.

Flash Media Server workflow example

The workflow depicted in Figure 1 (below) shows a typical content provider or retailer offering premium content licensed from other sources such as movie or TV studios. Different deployments will have different workflows; for instance, an enterprise or educational setting may or may not rely on an external CDN. In this example, Flash Player is the client runtime, but an equivalent workflow is also possible with Adobe AIR.

In the initial content preparation stage (step 1), the content provider receives raw content and encodes it using tools such as Adobe Media Encoder, Flash Media Encoding Server, or a third party encoder. The content provider also develops a video player, packages it as a SWF, and transfers it to the CDN along with the encoded content (step 2). The ingest process and distribution to edge servers is specific to each CDN and is not shown in this workflow.

Next, a consumer browses the content provider's web portal and navigates the library of available content (step 3). The web portal enforces the business logic—such as access controls—that vary

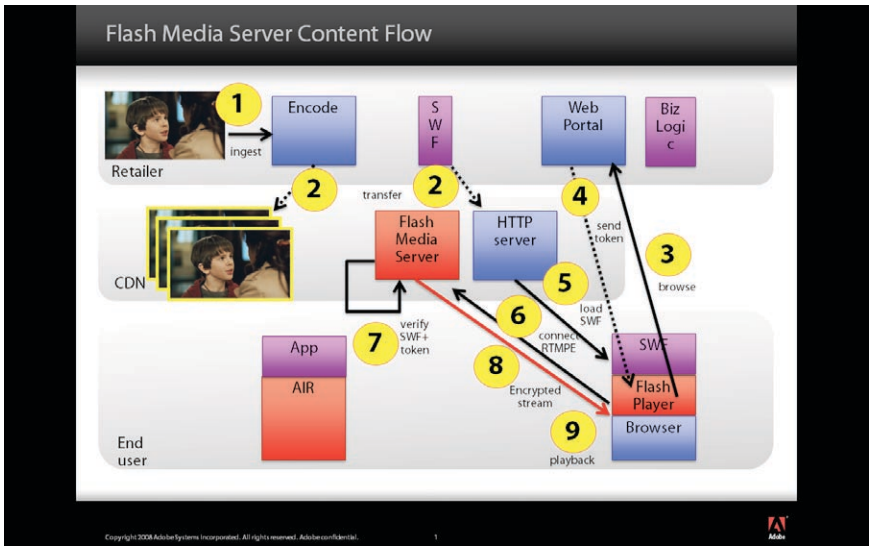
depending on the provider and business model. For instance, an advertising-funded business model may not need to identify the user, whereas a subscription business model must confirm a user's identity, and a pay-per-view business model typically requires an e-commerce transaction. The user's browser may optionally receive an authentication token (step 4) and connects to a CDN server to download the SWF (step 5).

The custom programs within the SWF application instruct the Flash Player to establish a secure connection using RTMPE (step 6). The CDN can configure Flash Media Server to reject connections that do not have the appropriate protocol. The Flash Player then sends the SWF verification hash and the authentication token securely over the encrypted channel. Flash Media Server verifies that the SWF is correct and unchanged, and checks for other security mechanisms such as valid tokens or geo-limiting (step 7).

If the request passes all checks, Flash Player will request Flash Media Server begin sending content. Flash Media Server encrypts it on the fly and streams content, to the Flash Player (step 8). The Flash Player decrypts the content as it arrives, renders it in the video player, then discards the video after the user has viewed it.

- A key security distinction of Flash Media Server is that it streams video directly to the Flash Player (step 9). This is in contrast progressive download, which temporarily downloads content to a user's computer. Flash Media Server and RTMPE never leaves content unprotected on a user's disk. This eliminates the possibility of a popular phishing attack that makes unauthorized copies of content temporarily cached on disk.

Figure 1: Secure video distribution using Flash Media Server



Persistent content protection with Flash Media Rights Management Server

Adobe Flash Media Rights Management Server offers more ways to monetize video assets while protecting them from misuse. Flash Media Rights Management Server lets you control how and where content can be distributed and viewed, providing end-to-end protection throughout the content lifecycle. It protects Flash Video files (in FLV or F4V format) streamed or downloaded to a supporting client. Currently, Adobe AIR supports playback of protected content, enabling rich Internet applications that run on Macintosh, Windows, or Linux platforms.

Flash Media Rights Management Server allows you to assign usage rules to content, supporting a wide range of business models, including video on demand (VOD), "all you can eat" subscriptions, anonymous advertising-funded viewing, download-to-rent, and download-to-own.

Flash Media Rights Management Server content protection features

Flash Media Rights Management Server and Flash Media Server can work independently or in combination. This section covers some of the salient differences between the two solutions. For more information on Flash Media Rights Management Server, please reference the white paper at *http://www.adobe.com/products/flashmediaserver/pdfs/FMRMS_whitepaper.pdf*

Independent of Transmission Protocol

Unlike Flash Media Server, Flash Media Rights Management Server makes content protection independent of the transmission mechanism. For example, Flash Media Rights Management Server can stream protected content via Flash Media Server using RTMP, progressively download content using HTTP, or download protected content in its entirety for local playback. You can create a complete distribution workflow with Flash Media Rights Management Server without using Flash Media Server.

Persistent content protection

Flash Media Rights Management Server protects content throughout the distribution chain. You can protect content before you transfer it to the CDN, reducing the security exposure that might result from keeping unprotected files on edge servers. The content remains protected even after users have downloaded and viewed it, providing ideal security for download-to-rent and download-to-own business models. Only consumers who have acquired rights for a particular piece of content can play it. This limits misuse and piracy, since copying or moving the file will not allow other viewers to watch it without the proper authorization.

Flexible usage rules

Flash Media Rights Management Server lets you create usage rules and assign them to content. For example, Flash Media Rights Management Server can enforce time constraints on content for rental business models; require playback of digitally signed playlists for advertising-funded business models; and bind content to a user account or user group for download-to-own or subscription business models. A compatible client such as Adobe AIR enforces these rules on the user's platform. For example, if you are renting content to consumers, you may specify a policy that grants a viewing period of a week. When the consumer acquires rights to a piece of content, Flash Media Rights Management Server sets the expiration date according to the policy in the content license. Once the viewing window expires, the client can no longer play the content unless it contacts the server again and acquires additional rights.

Flash Media Rights Management Server integrates with existing infrastructure, such as order management, e-commerce transactions, or subscription databases.

Offline access

Flash Media Rights Management Server gives you the flexibility to let consumers enjoy downloaded content even if they disconnect from the Internet. You can configure Flash Media Rights Management Server to issue a content license when consumers download content, allowing them to disconnect from the network and watch content at their convenience.

Comparison between Flash Media Rights Management Server and Flash Media Server

Both Flash Media Server and (FMRMS) offer security features that protect content from being stolen or altered. Both are suitable for several business models. Table 1 may help you decide which Adobe product to use to help secure your video distribution.

Table 1: Comparing business models and delivery models of Flash Media Server and Flash Media Rights Management Server

Business Models/ Delivery Options	Flash Media Server	Flash Media Rights Management Server
Electronic sell-through/download-to-own		x
Rental		x
Subscription	x	x
Advertising-supported	x	x
Corporate communications or education	x	x
Stream to Flash Player	x	
Stream to custom AIR Application	x	x
Download to custom AIR Application		x
Offline playback		x
Live video	x	

Summary

No matter what your business model and security needs for online video distribution, Adobe has you covered. With 98% of viewers using Adobe Flash technology to watch videos online, it is the overwhelming market favorite for delivering video on the web today. Using Flash Media Server and Flash Player is easy and convenient for consumers. Broadcasters and retailers can use the same content delivery networks and distribution technology they use today, with the added security features of Flash Media Server 3.5.

Flash Media Rights Management Server lets you protect and control access to premium commercial content with branded rich media applications that help generate new revenue or reach new audiences. It gives you the flexibility, reach, and development tools to develop a range of innovative business models, while persistently protecting content. With video playback applications built on Adobe AIR, consumers can enjoy access to more quality online media through an intuitive, convenient, and engaging interface, including playing content from their local content library.

Adobe is the leading brand in video creation, distribution, and control of video content. Let Adobe help you increase brand awareness, differentiate your offering from the competition, and create new revenue streams.

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

xxxxxxxx 7/09