



videofurnace

Delivering Secure IP Video

A VIDEO FURNACE WHITE PAPER

Table of Contents

3	Overview
3	Recent IP Video Security Threats
3	Key Areas of IP Video Vulnerability
3	Media Player
4	Browser-based Media Streaming
4	Data-at-rest
4	Video Furnace Solution
4	Encode and Encrypt
4	Eliminate Resident Players
4	Deliver Secure Streams
5	Conclusion

Overview

As video and streaming video make greater inroads into network computing environments, a clear and present danger has begun to emerge: security vulnerabilities. While no wide-spread exploitation of these IP video vulnerabilities has yet been reported, the breaches are serious and wide-spread enough to warrant extra vigilance. This paper outlines the chief areas of weak security in the majority of IP video platforms and the steps that Video Furnace has taken to ensure its products deliver secure IP video.

Recent IP Video Security Threats

While much has been made regarding browser and operating system vulnerabilities over the years, security and research analysts are only now coming to grips with the threats posed by network usage of IP video and audio. Vulnerabilities have been reported for Windows Media™ Player, Apple® QuickTime®, Firefox® media streaming and a number of unnamed open source media players and IP video streaming packages. Over the last three months, the following has been reported in *Computerworld*, *Network World*, *PC World*, *TechNewsWorld* and elsewhere:

- A QuickTime vulnerability allows scripting to run with full user rights without the user's knowledge. Because of the background nature of this security hole, a hacker could insert code to take over system resources, run full-blown hacker applications and collect or maliciously destroy data on the infected machine. In addition, security experts point out that iTunes® software, using similar full-user rights authority, could also become a security breach for unsuspecting users.
- Windows Media Player is vulnerable to attack by hackers through either the introduction of HTML code into files run by the less-restrictive media player or by exploiting user rights breaches in the player itself. These security holes allow hackers to gain access to other Windows resources and to phish for user credentials by easily faking the Windows login/logout sequences.
- A flaw in Windows security makes Firefox and Opera users open to attack through the operating system. In other words, even if users are running Firefox or Opera, streaming video or audio in these browsers may still allow the download and launch of malicious code.

In addition, in an address to the Black Hat USA 2007 hacker conference, David Thiel, senior security consultant with iSEC Partners, declared the firm had found significant faults in both commercial and open source media streaming programs. Thiel found some of the flaws particularly disturbing as they allowed the automatic launching of potentially malicious code. He declined to name the products because he is still disclosing the exploits to the software developers so they can develop and implement patches to fix them.

Key Areas of IP Video Vulnerability

An examination of the recent rash of video and audio IP security flaws shows that the majority of the security concerns center on these three areas: media player, browser and data-at-rest vulnerabilities.

Media Player

Because media players often are allowed access to operating-system level resources, they continually are exposed to threats from outside sources. In addition, to provide certain digital rights management and interface controls, the players must frequently run Java, HTML and other scripted code strings. While patches for evolving threats can be issued, with each new revision of the players new security holes may be introduced. As long as the media players are so intimately tied to the operating system or running in a less secure segment of the operating system, they always will be susceptible to security flaws.

Browser-based Media Streaming

Similar to the media player, browsers may be too closely tied to the operating system to provide full insulation from malicious code. In addition, unlike media players, these browser-based media streams may be automatically launched from any Web site using Java or HTML embedded in the page, providing virtually no protection from the launch of hacked or embedded malicious code.

Data-at-rest

Unencoded and unencrypted multimedia files stored on servers or local drives are susceptible to modification from outside rogue software including worms and viruses. In addition, these “open” files can become infected during transmission or prior to play, as the receiving players and media streamers are only expecting common media file types for processing.

Video Furnace Solution

Throughout the engineering and deployment of Video Furnace solutions, the company has made security and integrity of its delivery system top priority.

Encode and Encrypt

Throughout their lifecycle, media files are vulnerable to malicious attack—from inception, storage, delivery and playback. First and foremost, Video Furnace employs the strongest encryption available in the creation, storage and delivery of media streams: Advanced Encryption Standard. The AES strong encryption method was approved by the U.S. Department of Defense in 1997, and since its development in 1995 there has been no crack of the AES encryption method despite years of attempts. Because the AES system uses both variable length bit lengths for the encoding, and variable length keys for encryption and decryption, it is especially resistant to brute-force security attacks. As the Video Furnace system utilizes AES throughout the entire lifecycle of its multimedia delivery stream, the media streams themselves are highly resistant to tampering of any kind.

Eliminate Resident Players

Because commercial and open source players operate in an open and unsecured Internet environment, and many third-party providers develop player plug-ins for everything from visualizations to compression codecs, they are especially susceptible to hacking and malicious code.

Video Furnace has developed a micro-client viewing technology that automatically provisions the host (utilizing digital certification technology) upon request of the service. The request from the host is passed through a license manager before issuance. The license manager is of open design which allows user specific validations to occur before provisioning the host.

By removing the requirement to manually install a viewer at the host, the provider ***controls the process of placing the viewer in the host environment, changing it as needed, and removing it from the host when the session is terminated.*** This design completely removes any possibility of the media player being hacked by outsiders. The Video Furnace InStream™ player is not a browser plug-in, nor is it a Java applet. It is a standalone, runtime executable file that is separate from the browser. This unique design ensures that the stability of the viewing experience is independent of the stability of the Web browser. The Web browser is used to enable the video selection and subsequent automatic player delivery. Once the InStream player has been streamed, the user is free to close or minimize the browser, or surf to another site altogether, while continuing to enjoy the video experience.

Deliver Secure Streams

Because the Video Furnace stream is secured using AES encryption directly to the user’s desktop, brute force hijacking of the stream is extremely unlikely. The ability of the system to add an additional layer of security as validation is to invoke a “watermark” option on streams as well. With this exclusive system, the stream is watermarked with the end user’s IP or MAC address. This on top of AES encrypted streams provides not only security but media streaming tracking as well.

Conclusion

Media streaming security vulnerabilities will persist and proliferate if media player, browser and data-at-rest issues are not specifically addressed. Video Furnace, the leading provider of enterprise-class, mission-critical, secure video distribution, has employed specific and significant design criteria to ensure the safe delivery and deployment of IP video in network computing environments.

Work Cited

Jack Germain, TechNewsWorld, "Media Player Exploits: New Vectors, New Threats," September 26, 2007.

Greg Keizer, Computerworld, "Security Researcher Finds Flaw in Windows Media Player," September 19, 2007.

Jordan Robertson, Associated Press, "Media Players Have Significant Flaws," August 2, 2007

© 2007 Video Furnace, Inc. All rights reserved.

The information contained in this document represents the current view of Video Furnace, Inc. on the issues discussed as of the date of publication. Because Video Furnace must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Video Furnace, and Video Furnace cannot guarantee the accuracy of any information presented after the date of publication.

This paper is for informational purposes only. Video Furnace makes no warranties, express or implied, in this document.

Video Furnace and InStream are registered trademarks of Video Furnace.

Other product or company names mentioned herein may be the trademarks or registered trademarks of their respective owners.

Video Furnace, Inc.

Headquarters

14052 Petronella Dr. Suite 202, Libertyville, IL 60048, USA

Phone: 1.847.362.6800 **Fax:** 1.847.362.6866

info@videofurnace.com

www.videofurnace.com