Winter 12-8-2014

Active Authentication via Hiding Programs in Digital Contents

Fang Yu

Wei-Shao Tang

Yue-Zeng Lin

Wei-Ren Wang

ACTIVE AUTHENTICATION VIA HIDING PROGRAMS IN DIGITAL CONTENTS

Fang Yu, National Chengchi University, Taiwan, yuf@nccu.edu.tw
Wei-Shao Tang, National Taiwan University, Taiwan
Yue-Zeng Lin, National Chengchi University, Taiwan
Wei-Ren Wang, National Chengchi University, Taiwan

ABSTRACT

We propose a generic active authentication framework via hiding programs in digital contents, especially designed for H.264 / MPEG-4 AVC video formats. Besides using cryptography and steganography techniques, we bind a scripting language runtime as process virtual machine, giving the developer the possibility to design their own variant from passive authentication to active code execution.

Keywords: H.264, watermark, cryptography, steganography, runtime.

SUMMARY

With the digitalization of media, the improvement of video compression technique and the adaptation of the Internet, videos have become one of the most prominent mediums in the network age. However, due to its nature to be easily copied and distributed, creative workers easily become victims to the piracy. While corporations use proprietary digital rights management (DRM) to guarantee fair use of intellectual properties, individuals are seldom able to afford huge royalty. In the meanwhile, most of DRM techniques are frequently criticized for violating Kerckhoff's principle, i.e., a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Therefore, an alternative solution for public users is introduced in this paper. Using cryptography and steganography technique, authentication can be achieved with relatively low cost. Additionally, binding a programming language runtime as a callback, we can transform passive authentication to active executions, providing more flexibility on authentication via allowing programmers to develop their own variants.

Steganography means the art of concealing a message within another message. In the field of computer science, message is often viewed as bit streams, an atomic unit standing for message. To hide message in certain carriers, it is needed to know the properties of the carrier that may vary from one to another. We're particularly interested in H.264 / MPEG-4 AVC video compression format, due to its popularity on the Web. According to the survey mefeedia conducted, about 80 percent of videos on the Web are encoded in H.264 codec. For the message intended to be embedding, we adopt a public key cryptography algorithm to make sure that attackers pay high costs to use brute force to obtain the cipher text from the modified carrier. For situation where the embedded plain text is intended to be a program, we adopt Lua, a light, fast, interpreted programming language as the primary programming language for developers. Combined with its open source ANSI C implementation, one advantage of using Lua is that the execution runtime performs the same action on different operating systems and processor architectures. The data-hiding procedure starts with a special remuxer, where the plain text is encrypted using a public key, and then is divided to a series of bit streams and is later inserted into video packets. The seed number encrypted by a cryptographically secure pseudo-random number generator (CSPRNG) is attached to the header later. To execute programs while playing the embedded video, a special player is developed. The private key is first used to decrypt and obtain the seed number that is used to later extract bit streams from video packets. The original message can then be reconstructed and feed to the interpreter for execution. In the full paper, we first briefly introduce background knowledge required to design the toolkit (e.g. PGP encryption, H.264 / MPEG-4 AVC, CSPRNG and etc.), and then demonstrate how the toolkit is implemented along with a new web service: MIA for public users to embed their data in digital contents.

To sum up, we apply cryptography and steganography techniques to data hiding in digital contents, proposing a new mechanism with the aim of proving content owners the ability to claim digital ownership. We focus on H.264 video formats that have significant increasing popularity on the Web. Specifically, we investigate the properties of H.264 / MPEG-4 AVC, the concept of PGP software and public-key encryption/decryption, and apply it to our prototype system. Moreover, we bind a scripting language runtime to the player. Hence, the developer is allowed to design their own variants on hidden data (or programs) based on their requirement. The current technique used to embed messages in video satisfies integrity but cannot resist attacks/modifications on the video. An ongoing work is to replace its own implementation as modules that can be integrated with other data hiding techniques.