IGI PUBLISHING

ITJ 4565

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics,Volume 1, Issue 1
edited by **Chang-Tsun Li © 2009, IGI Global**

Efficient Forensic Analysis for Anonymous Attack in Secure Content Distribution

Hongxia Jin, IBM Almaden Research Center, USA

ABSTRACT

This article discusses a forensic technology that is used to defend against piracy for secure multimedia content distribution. In particular we are interested in anonymous rebroadcasting type of attack where the attackers redistribute the per-content encrypting key or decrypted plain content. Traitor tracing technology can be used to defend against this attack by identifying the original users (called traitors) involved in the rebroadcasting piracy. While traitor tracing has been a long standing cryptographic problem that has attracted extensive research, existing academia researches have overlooked many practical concerns in a real world setting. We have overcome many practical concerns in order to bring a theoretical traitor tracing solution to practice. The main focus of this article is on designing efficient forensic analysis algorithms under various practical considerations that were missing from existing work. The efficiency of our forensic analysis algorithms is the enabling factor that ultimately made the first time large scale commercialization of a traitor tracing technology in the context of new industry standard on content protection for next generation high-definition DVDs.

Keywords: *copyright; cryptography; digital video; encryption; forensics; piracy; traitor tracing*

INTRODUCTION

The advent of digital technologies has made the creation and manipulation of multimedia content simpler. It offers higher quality and a lot more convenience to consumers. For example, it allows one to make perfect copies. However this also enables easier piracy.

Unauthorized music and movie copying are hurting the profit of the record industry and the movie studios. It is highly desirable to develop techniques to protect the copyrighted material.

In this article we are particularly interested in business scenarios that involve one-way distributions, including pay-TV systems (Cable companies) or movie rental companies like Netflix, and massively distributing prerecorded and recordable media. Previous content protection system CSS (Content Scrambling System) protected DVDs with content encryption. The encryption key is shared among all DVD

players in the same manufacturer. However, content encryption cannot solve the content protection problem completely. Soon after CSS was introduced it was broken. The nightmare was that the system cannot be renewed in the sense that the compromised players cannot be revoked (excluded) from the system without hurting other innocent players. Lesson learned, new content protection systems are now based on broadcast encryption technologies (first introduced by Fiat & Naor, 1993) that enable a broadcaster to encrypt the content so that only a privileged subset of users (devices, set up boxes) can decrypt the content and exclude another subset of users. In this system, each decoder box is assigned a unique set of decryption keys (called device keys). A broadcast encryption scheme is defined to assign keys to devices and encrypt the content that can guarantee that only compliant devices can decrypt the content, without requiring authentication of the device.

Broadcast encryption is currently being used for content protection of recordable and prerecorded media (CPRM/CPPM) and is implemented in consumer electronics devices ranging from highly portable audio players that use Secure Digital Cards to top of the line DVD-Audio players supporting multiple channels, higher sampling rates and improved frequency response. The media, such as CD, DVD or a flash memory card, typically contains in its header the encryption of the key K (called media key) which is indirectly used to encrypt the content following the header. The media key is encrypted again and again using all the chosen device keys and forms a Media Key Block (MKB) which is sent alongside the content when the content is distributed. The device keys used to encrypt the media key are chosen in a way as to cover all compliant devices. It allows all compliant devices, each using their set of device keys, to calculate the same key K. But the non-compliant devices cannot calculate the correct key using their compromised keys. Thus the Media Key Block (MKB) enables system renewability. If a device is found to be non-compliant, a set of his device keys is compromised, an updated MKB can be released that causes a device with the compromised set of device keys to be unable to calculate the correct key K. This effectively excludes the compromised device from accessing the future content. The compromised device keys are "revoked" by the updated MKB.

There are various pirate attacks that can happen in the above broadcast encryption system.

In this article we are interested in anonymous rebroadcasting attack. Some legitimate users have instrumented their devices, and resell the movies by redistributing the decrypted movie itself or the per-movie decryption keys. For example, the attackers can setup a server that sells the media keys on demand. The attackers may also re-digitize the analogue output from a compliant device and redistribute the content in plain form. To defend against these types of anonymous attack, it seems one must distribute different versions of the content/key to different users. The content needs to be differently watermarked as well as differently encrypted.

Digital content watermarking/fingerprinting (Trappe, Wu, Wang & Liu, 2003) is a related field. Watermarks and fingerprints are unique labels/marks embedded in different copies of the same content. When an illegal copy of the multimedia content is found, the embedded watermark and/or fingerprint can be used for identification of the illegal users who distributed that copy.

Traitor tracing, an active forensic research area in cryptography, is a related but different field than digital content fingerprinting. It refers to a class of key management schemes that can be used to trace pirated cryptographic keys or pirated content. Notice that watermarking/fingerprinting technologies usually do not apply to cryptographic keys.

Furthermore, even if one needs to perform forensic analysis based on redistributed plain content, watermark/fingerprinting alone does not solve the problem by themselves. To meet our forensic analysis needs, the watermark has to identify the end user or allow us to derive the set of device keys used in the end user's device.