A Framework for Digital Watermarking Next Generation Media Broadcasts

Dominik Birk[†*] Seán Gaines[*] Christoph Wegener[†]

Abstract—**The Internet presents a problem for the protection of intellectual property. Those who create content must be adequately compensated for the use of their works. Rights agencies who monitor the use of these works exist in many juristictions. In the traditional broadcast environment this monitoring is a difficult task. With Internet Protocol Television (IPTV) and Next Generation Networks (NGN) this situation is further complicated.**
In this work we focus on Digitally Watermarking next generation media broadcasts. We present a framework which provides the ability to monitor media broadcasts that also utilises a Public Key Infrastructure (PKI) and Digital Certificates. Furthermore, the concept of an independent monitoring agency, that would operate the framework and act as an arbiter, is introduced. We evaluate appropriate short signature schemes, suitable Watermarking algorithms and Watermark robustness. Finally, the application of the proposed framework in other related scenarios is discussed.

Keywords: Next Generation Networks, broadcast monitoring, public key watermarking, IPTV, PKI, short signature

1 Introduction

The global acceptance of revolutionary services, such as IPTV [1] and NGN [2], is in the state of growth and impels broadcasters and media creators to evolve their existing infrastructures and services. IPTV, for instance, shows the potential to bring interactive content to the masses. Consumer applications such as interactive TV (iTV) [1] changes the modality of the TV set from being the source of one-way passive entertainment to a two-way interactive entertainment and communications model.
With the transition to digital media streams received over the Internet, new challenges loom. Today, the practices of recording, distribution and copying multimedia content is easy and straightforward [3]. Due to these facts, it is more and more difficult to enforce copyright and to safeguard intellectual property for broadcast media.
Digital Watermarking [4], which may be considered a form of steganography [5], attempts to address this problem by embedding information within the digital signal. The primary use of Watermarking is on digital signals that encode audio, image or video content. However, Digital Watermarking may be used for a wide range of applications such as copyright protection [6], fingerprinting [7], broadcast monitoring, advertising monitoring [8] and communication over covert channels [9]. It is debatable whether traditional Watermarking systems, which are based on disclosure of the key needed to embed and to detect the Watermark are generally suitable for proving ownership or authentication. Therefore, we established a framework based on asymmetric public-key cryptography which is used for exhaustive authentication with the help of *Blind Watermarking* techniques.
In addition to the traditional analogue, and newer digital, radio and television transmission means, programme broadcasts may also be received over the Internet. The *broadcaster* (BC) is an entity which broadcasts content for general consumption over their assigned channels, for instance an IP network (IPTV). In many jurisdictions broadcasters have regulatory obligations which attempt to protect the intellectual property [5] and copyrights of authors, songwriters, performers, actors, publishers, etc. Furthermore, in some jurisdictions there exists bodies charged with the defense of the rights of intellectual property and copyright holders and the calculation, charging and collection of performance royalties on the use of these protected works. Currently, there are several cases in which broadcasters cannot confidentially confirm that their royalties liabilities are correctly calculated. This is because they currently do not employ a viable automated system to measure what protected works are broadcasted, how often and when. Therefore a gap has opened up in the actual amount charged by the rights bodies and the correct payable royalties liability of the broadcaster.
This paper focuses on methods and procedures to close this gap and to support means for obtaining more detailed information about streamed content. A framework for authentication based on PKI for the parties involved is introduced, as is a framework for Watermarking rich media content. The main objective of these frameworks is to provide the ability to the broadcaster to be able to prove the amount of streamed media actually used to the agency responsible for monitoring broadcasters. This agency is called the *monitoring agency* (MA) and is

[*]VICOMTech Research Center, Paseo Mikeletegi 57, E-20006 San Sebastian, Spain
[†]Horst Görtz Institute for IT Security, Ruhr-University Bochum, Gebäude IC 4, D-44780 Bochum, Germany

charged with supervising broadcasting stations for purposes of calculating the royalties to be paid by broadcasters to the rights body. Monitoring agencies are often instructed by a *rights entity* (EX), which is a competent organisation charged with protecting the rights of intellectual property and copyright holders, and negotiating recompensation for the exploitation of these works.
However, this framework is in the interest of each involved party and attempts to address the needs of all parties. The broadcaster can be sure that it is being charged fairly. The monitoring agency can offer services and get paid for doing so. The rights entity can perhaps calculate that a broadcaster should pay more, or less, royalties than they are actually paying. For each party a substantial advantage can be seen by implementing such a framework.

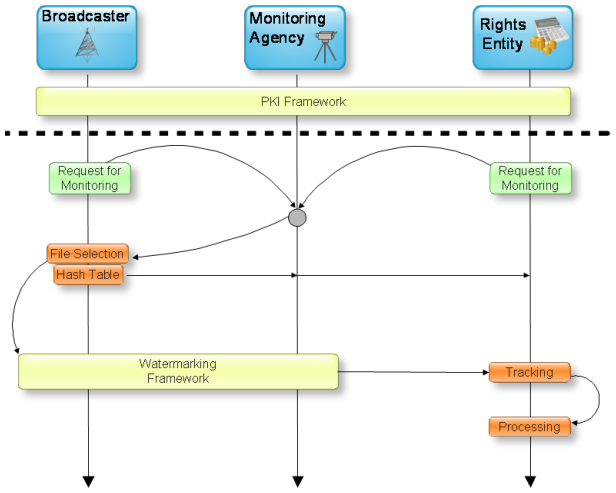

Figure 1: General Framework Overview

2 Framework Overview

A general overview of the framework with its three parties can be seen in Figure 1. It makes use of two additional frameworks, the PKI and the Watermarking Framework. The PKI Framework (section 4), is used for establishing a trust network between all of the involved entities. It makes use of a root Certificate Authority (CA) in which each participating entity must trust.

In order to establish a working PKI, each of the parties has to process one or more protocol steps. The PKI establishment has the purpose of distributing authenticated private and public keys utilising Digital Certificates. To start the process of monitoring, a "Request for Monitoring" is sent to the monitoring agency. Afterwards, broadcaster selects a piece of content which he wants to stream and computes the corresponding hash table. This hash table is carried over a secure and authenticated channel to the MA as well as to the EX. Subsequently, the broadcaster initiates the process defined by the Watermarking Framework.
The Watermarking Framework (see section 5) specifies procedures for Watermark embedding, retrieval and verification of Watermarks in media streams. The broadcaster will sign the stream which is about to be broadcasted with his private key. Then the corresponding signature is embedded into the media stream with a known Watermarking technique. Further on in the process, the monitoring agency will extract the Watermark and verify the signature. Therefore, the agency may be sure that only the original broadcaster broadcasted the media content, due to the fact that additional security metadata, such as timestamps and identifiers, are used. Additionally, EX can also verify the signature in order to prevent abuse by the MA.
The objective of the whole framework is to let the broadcaster mark the file stream uniquely but also provides the monitoring agency with the possibility to identify the broadcast stream and therefore the corresponding broadcaster. In this paper we focus on the novel IPTV broadcasting infrastructure [2]. However, our framework should be applicable to any broadcasting infrastructure irrespective of the underlying distribution network.

3 IPTV Overview

IPTV is a new method of delivering digital video and audio content across IP networks [10]. Today, the industry is going through a profound transition, migrating from conventional TV to the era of digital technology. IPTV technology provides several advantages but service providers face a set of specific barriers, namely the availability of sufficient network capacity, especially in the last-mile or local loop section of the broadband network that lies between core telecommunications network, or back-haul trunks, and the end-user. There are currently six principal types of broadband access networks which have sufficient capacity and scalably to meet the bandwidth requirements of IPTV:

- Optical Fibre
- Digital Subscriber Line (DSL)
- Cable TV
- Satellite Broadband
- Fixed Wireless Broadband
- 3G Mobile Data Networks

Several different applications can be provided by IPTV service providers over a broadband connection, however the two key IPTV applications typically deployed by service providers are broadcast digital TV and content on demand (CoD). In this paper we only focus on digital TV broadcast.

Security is the number one priority for IPTV service providers because video content producers are reluctant to grant license rights to distribute premium content over digital networks unless there are effective mechanisms in place, which will secure that content. There are a number of IPTV content protection schemes available on the market. These protection schemes fall into two broad categories: Conditional Access (CA) and Digital Rights Management (DRM) environments. The CA system is primarily responsible for ensuring unauthorised access of the IPTV service, while the DRM system enforces content owners business models and granted usage rights.

4 PKI Framework

Trust forms the basis of all communication, be it physical or electronic. In the case of electronic communication, building trust is quite difficult as the identity of the other entity remains concealed. In our specific case, trust is also the foundation for the calculation and collection of royalties. The three entities, the rights entity, the broadcaster and the monitoring agency, need to trust the CA. Therefore, a PKI needs to be established which provides procedures to generate, distribute, and utilise keys and Certificates and so helps to build up a trust relationship. We propose a single-CA architecture which makes use of a superior independent Certificate Authority. The CA must not be involved or integrated in metering and should be independent and impartial. Within the single-CA architecture, all entities trust the CA and therefore can validate and verify each others Certificates and then communicate. In later communications, the CA need not be involved.
After a successful PKI-establishment, the broadcasting entity could sign a message and send it to the monitoring agency or indeed to the rights entity and both entities could be assured, that the message was sent by the broadcaster.

5 Watermarking Framework

The Watermarking Framework specifies the communication protocol between the broadcaster and the monitoring agency in which the rights entity is not involved. Furthermore, the Watermarking Framework provides a detailed insight into procedures for creating, detecting, extracting and verifying the Watermark.

5.1 Overview

The chief characteristic of a traditional Watermarking scheme for copyright protection, or DRM, is that the Watermark cannot be separated from the medium without knowledge of a secret value. We, in our specific case, target on another characteristic: sender authentication. It should be possible to identify the broadcasting station unambiguously and show exactly who broadcast what stream and when.
Therefore, our Watermark information contains a digital signature issued by the broadcaster that definitively identifies the broadcaster. Each entity that receives the broadcast stream and owns the corresponding broadcaster Certificate, can clearly verify the distributed stream with the help of the corresponding PK.

5.2 Signature Schemes

A principal requirement to all Watermarking systems is the need for a small Watermark. The larger the Watermark, the larger are the chances for adversely affecting the quality of the streamed media. Therefore, the signature scheme output has to be as small [11] as is possible to be able to embed the Watermark as often as possible and to be repeated multiple times throughout the stream. While the typical RSA 1024-bit signature output is large, several alternative schemes were researched.
The Nyberg-Rueppel ([12], hereafter NR) signature scheme focuses on the size of the input and output and is a DSA-like signature with message recovery. The drawback of this signature type, the fixed length of input, is not given in our case because the message m (see (1)), which is used for exact identification of the stream, is always brought to a fixed length through a given hash function. NR is perfectly suited to messages shorter than ten bytes but leaves the question of dealing with short messages, of say fifteen bytes, unanswered. In our specific case, the hash to be signed is exactly 10 bytes long and brings only a marginal risk of collision. Message recovery [13], another characteristic of NR signatures, provides means so that the original message can be extracted out of the signature.

5.2.1 Short Hash Methods

Hash functions are often used in digital signature algorithms. The message m that is about to be hashed, in our case, consists of an identifier string *ID-str* concatenated with an ID number *ID-num* and an unique times-tamp *ID-time*:

$$m = \textit{ID-str} \,||\, \textit{ID-num} \,||\, \textit{ID-time} \qquad (1)$$

The ID-str could be represented through the name of the media content, for instance. The ID-num could be an identification number. The ID-time is a unique timestamp which prevents replay-attacks. This means, that an adversary may not record the stream and broadcast it later again on an authorised channel which is also monitored.

5.2.2 Hash Table for Verification Purposes

A hash table *ht* in our specific case is a data structure that associates the hash value with ID-str, ID-num and ID-time. The hash table contains several important attributes and is essential for the verification process by the MA.
Transferring the hash table *ht* to the MA, can be compared to the cryptographical *commitment scheme*, visualized in Algorithm 1.

Algorithm 1 Secure and Authentic Hash Table Distribution

Summary: during the *commitment phase*, the hash table is transferred to MA and EX. During the *opening phase*, BC proves to MA and EX that he is broadcasting one of the items in the hash table.

1. ***commitment phase***:

   1. BC $\longrightarrow$ MA: $\text{enc}_{PK_{MA}}(\text{sign}_{SK_{BC}}(ht))$
   2. MA $\longrightarrow$ EX: $\text{enc}_{PK_{EX}}(\text{sign}_{SK_{BC}}(ht))$

2. ***opening phase***:

   1. BC $\longrightarrow$ MA: $\text{watermark}(\text{sign}_{SK_{BC}}(hs))$
   2. MA: extract *signature* from stream with the help of beacon
   3. MA $\longrightarrow$ EX: $\text{enc}_{PK_{EX}}(\text{sign}_{SK_{BC}}(hs))$

The prover, respectively the BC, sends the "commitment" in form of the hash table *ht* to the verifier (the MA). MA will forward the signed hash table to the rights entity but encrypts it with the corresponding PK_{EX} in order to guarantee secrecy which is needed to prevent other parties from viewing the hash table. This can be seen as the *commitment phase* and takes place directly after having chosen the file to be streamed. The encryption is necessary due to the possibility that the hash table of a potential business rival might be seen by another party. Later, after broadcasting the media content, the verifier can scrutinise, with the help of the message recovery characteristic of the signature, whether the BC broadcast the content correctly or not (*opening phase*).

5.2.3 Case Study: Video Broadcaster

The *Internet Movie Database (IMDB)* [1] published interfaces for several systems to access the IMDB locally. For our case study, we downloaded the complete IMDB title textfile which contains currently 1.206.730 different movie titles. We used the movie title as a ID-str and created a unique number used as the ID-num. The time-stamp ID-time was the current date parceled as a unixtimestamp. An example assignment between unixtimestamp and normal time can be seen in (2).

$$05/07/1982@00:00 \Longrightarrow 389592000 \tag{2}$$

For instance, in our simulation, m looked like this:

$$\text{m} = \underbrace{\text{Title A}}_{\textbf{ID-str}} \;||\; \underbrace{23754}_{\textbf{ID-num}} \;||\; \underbrace{534056}_{\textbf{ID-time}} \tag{3}$$

We created 1,206,730 different messages m and subsequently hashed them with MD5 and SHA-1. Afterwards, we extracted the first 10 bytes which satisfy the first 20 characters of the output HEX value. No collisions were detected for both hash functions, MD5 and SHA-1, even with only using the first 10 bytes of the hash-sum.

$$hs = [0...9]hash(m) \tag{4}$$

Finally, a theoretical possibility to create a 2nd-preimage attack on our used short hash methods remains. Because of the reduced length of the hash value, our methods don't have the complete potential strength of 2^{160} (SHA-1) respectively 2^{128} (MD5) 2nd-preimage resistance. The search space would be reduced to 2^{80} respectively according to the birthday paradox on 2^{40}.

5.3 Suitable Watermarking Algorithms

In our specific case, the Watermark should have special control characteristics which are required to guarantee the ability to verify the embedded signature by the monitoring agency.
Spread-spectrum [14] technologies establish secrecy of communication by performing modulation according to a secret key in the channel encoder and decoder. Our specific scenario does not focus on secrecy but on authentication. Therefore, the beacon used for encoding and decoding, only contains the information how to process these steps. The beacon is not a secret value.

5.3.1 Proposed Watermarking Algorithm

Basically, a Watermarking system for our purposes can be described by a tuple $\langle \mathcal{O}, \mathcal{S}, \mathcal{W}, \mathcal{H}, \mathcal{P}, \mathcal{G}, C_S, E_H, D_H, V_P \rangle$ where $\mathcal{O}$ is the set of all original data, a video stream for instance. The set $\mathcal{S}$ contains all secret keys needed for creating an unforgeable signature. $\mathcal{W}$ represents the set of all Watermarks (signatures, in our case) and $\mathcal{H}$ the

[1] http://www.imdb.com

set of all beacons. Beacons in our scenario are markers that signify the presence and start of a Watermark bit sequence in the signal. The beacon substitutes the key in normal Watermarking systems. $\mathcal{P}$ describes the set of public keys which are needed to verify the signature and $\mathcal{G}$ represents the set of Certificates issued by the CA.
Four functions are described as followed:

$$C_S : \mathcal{O} \times \mathcal{S} \longrightarrow \mathcal{O} \tag{5}$$
$$E_H : \mathcal{O} \times \mathcal{S} \times \mathcal{W} \times \mathcal{H} \longrightarrow \mathcal{O} \tag{6}$$
$$D_H : \mathcal{O} \times \mathcal{H} \longrightarrow \mathcal{W} \tag{7}$$
$$V_P : \mathcal{W} \times \mathcal{P} \times \mathcal{G} \longrightarrow \{1, 0\} \tag{8}$$

C_S focuses on creating the corresponding Watermark through a signature. E_H describes the function for embedding the Watermark and D_H respectively the function for extracting it. Furthermore, V_P stands for the verification function needed to check if the Watermark is valid. The Watermark w is created with

$$w = sign_{SK_{BC}}(hs) \tag{9}$$

and outputs a short bit-string which contains the signature of the reduced hash-sum. See (4) for further details about the reduced hash-sum hs.

5.4 Embedding the Watermark

In this subsection we focus on the embedding process of the signature/ Watermark. Hartung and Girod proposed in 1998 [15] a method which focuses on Watermarking MPEG-2 video data. We adopt the proposed methods for our purposes of embedding the signature into a given video broadcast stream. For further information, the interested reader is referred to [15].

5.5 Retrieval of the Watermark

The proposed methods rely on *Blind Watermarking* techniques and therefore do not need the original video stream in the retrieval process. For further information, the interested reader is referred to [15].

5.6 Verifying the Signature

It is possible for the monitoring agency to verify the signature which is represented by the extracted bit sequence. The method V_P verifies the signature with the help of the corresponding public key and Certificate. The used public key for verifying is taken from the Certificate in order to be sure, that only the public key belonging to the correct broadcaster is used.

6 Conclusions and Future Work

The schemes proposed in this paper may be viewed as attractive to both broadcasters and rights agencies. This model provides the broadcaster and the rights entity with an automated and trust worthy method for measuring the exploitation of protected works. The paper introduces the concept of an independent third party that monitors and balances the interests of the broadcaster and rights entity. We discuss the rapidly evolving technologies

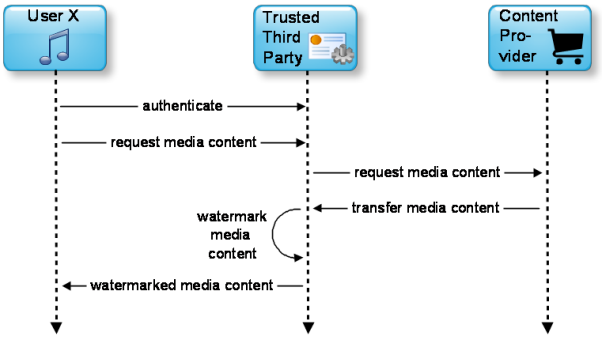

Figure 2: Abstract Proposal for DRM-substituting Business Model

and distribution models faced by the entertainment and broadcasting sectors. Then we discuss next generation media distribution using IPTV as an example. We evaluate established short signature schemes, such as Nyberg-Rueppel, that could be integrated into a final system.
Our model could function as a compliment, or an alternative, to established DRM models.
Therefore, in Figure 2 we propose an exemplified scheme which could substitute current DRM models. If a user wants to buy a media content (audio, video or image content) from a content distributor, the TTP handles the whole process. The request for the specific media content gets proxied by the TTP for providing anonymity. Afterwards, the content is Watermarked by the TTP with a user-specific signature and sent back to the user. This means, that the content provider will never get the knowledge of the user's secret key.
Clearly, Watermarking has a number of characteristics that make it an ideal technology for enabling a variety of media distribution business models. However, historically robustness has been a chief weakness of Digital Watermarking techniques.
A variant of our model could be used by existing online music services to modify their current DRM schemes toward an intellectual property preserving framework based on personalised Watermarks. Digital Watermarking schemes present an alternative to regulatory measures. Although not covered in this paper, the current body of national and European law provides legal protection for Watermarking and Digital Certificate technologies. A robust Digital Watermark can jump the analogue hole. This might mitigate the need for Broadcast Flags, TPM like chipsets or signal degradation on playback device to be mandated by law.
State of the art Watermarking techniques have taken substantial steps forward in addressing the issue of robust-

ness. Currently, the big four record labels rely on modern robust Watermarking algorithms to sell DRM-Free MP3 files through the Amazon MP3 store. There is a direct linear relationship between the robustness of a Watermark and the size of its payload. High definition content presents the ideal conditions to improve Watermark robustness. It has a greater than linear increase in size over standard definition. Therefore there is a greater quantity of available data in the signal to embed a complex and robust Watermark.
A Digital Certificate can be used to enter into a contract. A media file Digitally Watermarked with a value derived form a Digital Certificate may be viewed as a type of Smart Contract. This provides the distributor with a means to trace the file to the purchaser, should it appear on P2P networks. More importantly, the act of signing the media file motivates the consumer not to make an unauthorised copy of the file. Ideally the incentive to the consumer would be lower prices. The benefit to the distributor would be increased sales due to reduced piracy.

References

[1] Gerard Driscoll. *Next Generation IPTV Services and Technologies*. Wiley-Interscience, 2008.

[2] Neill Wilkinson. *Next Generation Network Services*, volume 1. Wiley & Sons, 2002.

[3] M Peitz and P Waelbroeck. Piracy of digital products: A critical review of the economics literature. cesifo working paper series no. *Information Economics and Policy*, (1071):2003, 2003.

[4] Ingemar J. Coxy, Joe Kiliany, Tom Leightonz, and Talal Shamoony. A secure, robust watermark for multimedia, 1996.

[5] Chun-Shien Lu. *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. Idea Group Publishing, 2005.

[6] W J Dowling and F M Boland. Watermarking digital images for copyright protection. pages 250–256, 1996.

[7] D Kirovski, H Malvar, and Y Yacobi. A dual watermarking and fingerprinting system. Technical report, ACM Multimedia, 2001.

[8] Jian Zhao. Applying digital watermarking techniques to online multimedia commerce. In *In Proc. of the International Conference on Imaging Science, Systems, and Applications, Las Vegas*, 1997.

[9] Zbigniew Kotulski Wojciech Mazurczyk. Covert channel for improving voip security. In *Advances in Information Processing and Protection*, 2007.

[10] Nigel Seel. *Business Strategies for Next-Generation Networks*. Auerbach Publications, 2007.

[11] David Naccache and Jacques Stern. Signing on a postcard. *Lecture Notes in Computer Science*, 1962:121–??, 2001.

[12] Kaisa Nyberg and Rainer A. Rueppel. A new signature scheme based on the dsa giving message recovery. In *Proceedings of the 1st ACM CCCS*, Fairfax, 1993. ACM.

[13] G. Ateniese and B. de Medeiros. A signature scheme with message recovery as secure as discrete logarithm. 1999.

[14] Ingemar Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 1997.

[15] Frank Hartung and Bernd Girod. Watermarking of uncompressed and compressed video. *Signal Processing*, 66(3):283–301, 1998.