Beyond Web Intermediaries: A Framework for Securing Digital Content on Client Systems

Stella C. Chiemeke, *Member*, *IAENG* and Olumide B. Longe

***Abstract*—The move to begin to place liabilities for copyright violations on internet intermediaries such as ISPs and Cyber Cafes as a result of contents allowed through their networks is a welcome development in the fight against copyright violations and piracy of digital contents. Beyond this however, experts must also realize that consumers of content have unguided opportunities to exploit digital content for undue gains once placed at their disposals. This is particularly possible as a result of the intrinsic properties of digital contents when compared to analog contents such as newspapers and transmissions from satellite cable stations. For example, multiple replications of digital contents can be carried out in the comfort of a client's home using modern technologies such as CD-R/W or burners without degradation in quality. To counter this threats, new security technologies are required that persistently protect content throughout its lifetime. Conditional Access Systems (CAS) has been used to protect content delivered over cables. We present a framework for an analogous protection system for digital content on client systems as a viable technique for protecting digital content that have passed through Internet intermediaries.**

***Index Terms— Digital rights, Content protection, Metadata, Copyright, Web intermediaries*.**

I. Introduction

The threat from piracy is very real -and very expensive. The alarming rate at which software piracy is taking place worldwide and in Africa in particular as well as its attendant effects on developments in information technology calls not only for serious concern but also the development of technical means by which it can be curbed. In [3], the development of an E-mail encryptor for securing mailing addresses from web crawlers at the intermediary level was proposed. As a result of the limitations involved in controlling what customers do with Internet contents of all types, content owners are reluctant to release valuable content in digital format because they fear for the unauthorized usage of their content. Napsterization still being very fresh in their memories.

Technology is available that enable content providers provide authorization and access control to ensure that only paying users can access content. They can also use encryption to protect content during transport [2]. The major challenge therefore is how to control what customers do with the purchased or available content once it reaches their computing facilities. Protecting digital content has to go beyond the prevention of illegal file sharing common in the musical world. Current efforts must embrace the development of techniques that can alter the paradigm of content owners so that they perceive the distribution of digital content over the Internet as an opportunity rather than- as a threat [1].

A. Digital Rights

Digital rights refer to copyright and related rights over digital contents (digital contents can be text (data), audio, and video streams in digitized version). The goal of digital content protection can be summarized as the identification/definition of digital rights and the implementation of digital content usage rules using proven digital content management techniques.

II. CONTENT PROTECTION OVER CABLES

Conditional Access Systems (CAS) popularly implemented using decoders Set Top Box (STB) was developed mainly to protect content delivered over cable and satellite networks and displayed on television (TV) sets. In this technique contents are transmitted and delivered through a STB that is secured using Smart cards. The smart card, which is "owned" by the consumer, is a Tamper-Resistant Device (TRD), as are some security-sensitive parts within the STB into which the smart card is inserted (e.g. the crypto modules). The STB stops functioning completely when the smart card is removed [5].

A. Principles for Implementing Protection over Cables

In protecting contents over cable, the content is encrypted before being sent over the network and the encryption keys change frequently. At start-up, the network authenticates both the smart card and the STB hardware. When a client is interested in particular content, the client sends a request to the content provider who checks the request against a policy database. When the client is authorized to receive the content, the content is streamed and the correct decryption keys and key

Manuscript received August 21, 2006.

S. C. Chiemeke is with the Department of Computer Science, University of Benin, PMB 1154, Benin City, Nigeria (phone: +2348023158911; e-mail: schiemeke@ yahoo.com).

O. B. Longe is with the Department of Computer Science, University of Ibadan, Nigeria. He is presently a doctoral student of the University of Benin, Benin City, Nigeria. (e-mail: olubab@excite.com).

updates are sent over a secure connection initially set up between the content provider's server and the customer's smart card. The principle is illustrated in Figure 1.

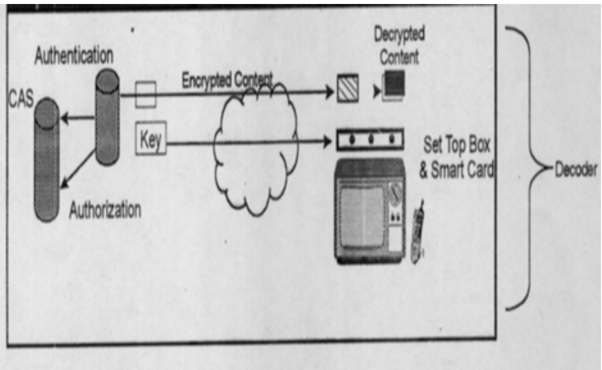

Fig. 1: Conditional Access System for Distributing Digitized Content Over Cable

Usage control after the content download is fairly easy. The STB usually has only an analog output interface to a TV. Although the STB is on the customer's premises, it is largely controlled by the smart card and the fact that the STB are tamper-resistant. The analog output could be used as a source for pirated copies, although this would result in serious degradation from digital to analog quality (as opposed to digital copying where degradation in quality does not occur). The experience is the same when content is distributed via traditional TV and Video Tapes.

B. Developing Analogous Protection For Internet Content

The development of an analogous protection system for contents downloaded via a client PC is a much bigger challenge, as the PC is an open platform over which the content provider has little or no control over. The content provider must, as a matter of necessity, take additional measures to control the usage of the digital content after it has been stored on the end user's system. Traditional CAS will not suffice in this case. An emerging trend is for clients to increasingly deploy client networks to connect to the Internet via Digital Subscriber Line (DSL) rather than connecting a single computer or STB. It is possible for a user to buy or license content that can then be accessed on different devices within one network without losing the protection and control over usage of content and without the need to pay a separate license fee for each device on the network. An analogous content management framework for client systems is depicted in the figure below.

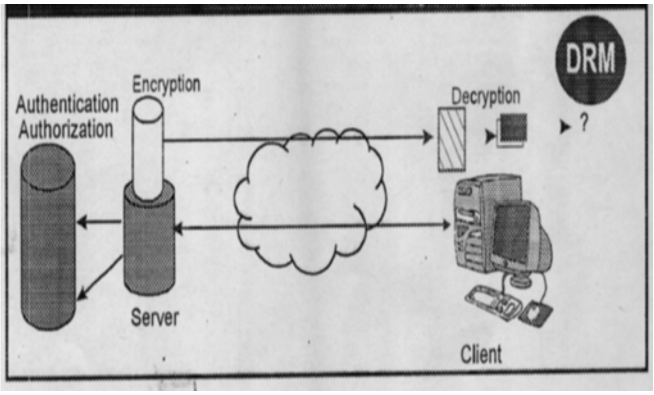

Fig.2: System for Distributing Digitized Content Over Client Systems

III. BUILDING BLOCKS FOR THE ANALOGOUS SYSTEM

To be able to express these rights as schemes in a machine-readable form, will involve taking advantage of Digital Right Languages (DRL). The other building blocks for this protection scheme are encryption, digital watermarking and usage rules. Usage rules will specify whether a client is allowed to make copies of the content possibly a limited number of times, as well as the extent to which contents can be replicated, rendered or forwarded to other users. Other possible rights include ***play, print, save, modify, edit*** etc. [4].

A DRLs

DRLs have been developed to express complicated digital content usage schemes in machine-readable formats. DRLs include eXtensible Rights Markup Language (XrML) and the Open Digital Rights Language (ODRL). Both of them are based on the eXtensible Markup Language (XML) platform designed for use in fixed and mobile solutions.

B. Watermarking

Digital watermarking technology falls within the field of digital signal processing. The aim of a digital watermark is to insert information into digital data, such as audio, video or image files, in a way that is imperceptible to the human eyes or ears yet detectable by compliant electronic equipment. Most watermark detection processes require knowledge of additional information which can be referred to as a "key". Watermarking keys are always symmetric in the sense that the same information is used for watermark insertion and detection. Possible applications for digital watermarking technology in the context of anti-piracy include:

(1) **Digital Signature**: In which digital watermarks are used to identify the owner of the digital content. The watermark then persistently binds the content to the copyright owner.
(2) **Fingerprinting**: In this case the watermark identifies the user/buyer of the protected content. Fingerprinting can help to trace the origin of illegal copies of copyright-protected content.
(3) **Copy Control**: Information related to usage rights and copyright can be included in the watermark and in this way be persistently attached to the content. These rules can include save, copy, modify, copy once, never copy, edit etc.

IV. PROPOSED ARCHITECTURE FOR CONTENT PROTECTION

The architecture is based on a separate distribution chain for encrypted content on the one hand, and for usage rules and the decryption key on the other. Encrypted content together with a small amount of metadata is digitally signed and stored on a web download or streaming server. Metadata is descriptive data associated with the content. It may vary in depth from merely identifying the content title or providing descriptive information to populate an electronic program guide, to providing business roles detailing how the content may be displayed, copied, or sold.

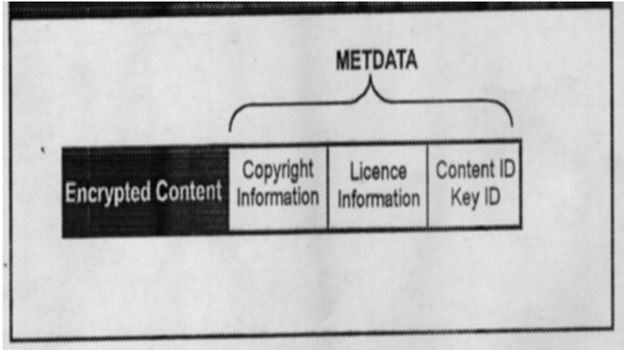

Fig.3: Streamed Media Packaged With Encrypted Content and Metadata

The metadata also provides the information necessary to retrieve the correct usage rights and the keys for decrypting the content. The combination of usage rules and the correct key to decrypt the content would in this architecture depict the license. The framework is shown in Figure 4.

A Usage Rules for Framework Implementation

In Steps 1 and 2, the usage rules are determined and stored together with content on a license server. At the same time, the digital content is encrypted, packaged with the correct metadata and then stored on a content distribution server. In Step 3, a client retrieves the encrypted digital content together with the metadata. From the information in the metadata, the client application detects that a license is required to be able to decrypt and render the content. If no appropriate license is found on the client device, the license information in the metadata redirects the client application to a license server (Step 4).

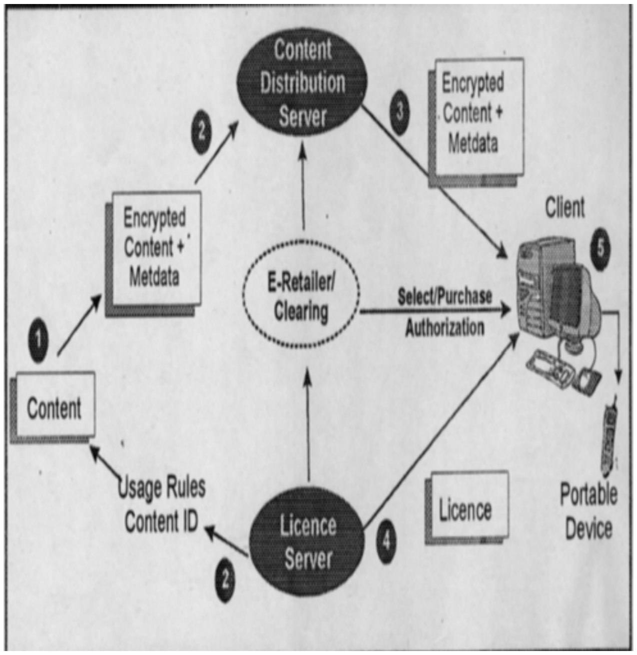
Content Distribution Server
Encrypted Content + Metdata
Encrypted Content + Metdata
Client
E-Retailer/ Clearing
Select/Purchase Authorization
Content
Usage Rules Content ID
Licence Server
Licence
Portable Device
1
2
2
3
4
5

Fig.4: Framework for Securing Digital Content on Clients' System

After the client has been authenticated and authorized (related to payment), the appropriate license is downloaded. This license is encrypted with a key that is unique to each client. The protocol used to protect license exchange is proprietary, but is often based on public key encryption techniques. The license contains the usage rights and the decryption key for the digital content. Once the client has the correct license, the application can decrypt and render the content. The content can also be exported to a portable device (Step 5).

Depending on the individual (proprietary) solution, there can be an additional functional element as indicated by the dotted lines in Figure 4. This element can be an ***e-Retailer***, which provides the interface to the client possibly delivers promotional materials and directs the client application to the correct content server. It can also be an entity involved in payments, which can act as a clearing house for license settlement. This architecture makes it possible to issue different licenses corresponding to different usage rights (and at different prices) for the same encrypted content.

V. CONCLUSION

As with every other security measure, protecting digital contents comes at a cost. A trade off must be made between security, strength, cost and ease of use. Accordingly the approach adopted in this paper will make it difficult and costly to break the system security and minimize hacking opportunities for attackers. In addition to cost and ease of use, standardization is an important factor for the successful technologies. Users will be unwilling to download a separate player with its own solution for each content provider; a cross platform standard with seamless operations will have to be agreed on.

VI. RECOMMENDATION

In their bid to compensate content owners for copyright infringements, some countries are seriously considering imposing levies on digital equipment, such as MP3 players, CD writers and, in the future, perhaps even on PCs, to compensate for revenues lost as a result of copyright infringement of digital content. The rationale is that content distributed in digital format are susceptible to unauthorized copying. The levies are computed based on an estimated average number of copies to be made per user device. Such levies increase the price of consumer electronic equipment and thereby hamper swift market adoption of new broadband services. This will be particularly pathetic for the developing world where governments are trying to device measures to make Internet connectivity and PCs available at reasonable cost to their populace.

Another consequence will be that people who do not make illegal copies are charged along with those who do. It becomes a case of “when the wicked suffers, the righteous will partake in it”. To overcome this impending negative retribution, we recommend content protection solutions such as the ones for which a framework has been proposed as more appropriate deterrents and alternatives for the protection of copyrights of digital contents especially those shipped to countries where piracy of every sorts is on the increase. We believe that when this framework is applied in the design of content protection systems, copyright levies as being insinuated will be abolished as they are not only anti-progressive for technology but also leads to double compensation for content owners.

REFERENCES

[1] Moffaert, E (2003); "Digital Rights Management" Retrieved August 2006 from http://www.alcatel.com/document

[2] Longe, O. B.(2004): Software Protection and Copyright Issues in Contemporary Information Technology. *Thesis Presented for The Award of a Master of Technology Degree in Computer Science at the Federal University of Technology, Akure*, Nigeria.

[3] Longe, O. & Chiemeke, S. (2006). The Design and Implementation of an E-Mail Encryptor for Combating Spam Mails from the Sending End. *Proceedings of the International Conference of the International Institute for Mathematical and Computer Sciences*. Covenant University, Ota Nigeria. June, 2006

[4] Renato, I. (2002); Open Digital Rights Language (ODRL) Version 1.111. IPR Systems, Retrieved July, 2006 from http://www.w3.org/TR/odrl/, http://www.alcatel.com/document

[5] Schneier, B. (1996): Applied Cryptography, Protocols, Algorithms and Source Code in C. Yorkshire; John Wiley Publishers.