ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

PREVENTION METHODS OF DDoS ATTACKS

MythiliBoopathi[1], Siddhant Vibhandik[2], Nitika Sinha[3]
[2,3]MCA Student, School of Information Technology and Engineering, VIT University, Vellore 632014
[1]Assistant Professor (Selection Grade), School of Information Technology and Engineering,
VIT University, Vellore 632014.
Email: siddhantv03@gmail.com

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract:

The invention of digital media plus Internet is changing our lifestyle drastically. Together they make it possible for numerous service providers to offer their digital media on the web and to sell them to end-clients and reach out to the audience efficiently. Due to this, clients can able to shop, read, watch movies, play online multiplayer games and even watch live matches or TV content. Digital Rights Management (DRM) is an anti piracy system for protecting the interests of the content developers in growing era of digital content and demands for digitalization of contents. DRM can be classified into two models un-tethered and tethered, these model focuses on management of payment and usage rights.

This paper analyzes and compares these two models which will be helpful in further research.

I. Introduction

Digital Rights Management is [3][4] system which prevents unauthorized redistribution of software, games, music, etc. The need for DRM is constantly increasing among digital content developers as online piracy of music, movies and cracking of software, games, etc are continuously hampering the legitimate earning, interests and support for the content developers.

Some DRM Techniques:

- Restrictive License Agreements
- Encryption based
- Online Authentications
- Product Keys
- Hardware bounded.

II. LITERATURE SURVEY

Common DRM parts for un-tethered & tethered model:

Basic functional parts of [5] both systems are essentially the same here. Content encryption keys: Keys used to encode content that are required at the client side to decode and get to that data or content. In DRM, the decoding key for one substance component is bundled with corresponding usage rules in an encrypted part named license. The keys utilized for encryption are unique to every end client.

- Packager: This network-side component is capable for content encryption with the content encryption key, for arranging information into a compartment as per a pleasing arrangement, (for example, the Worldwide Organization for Standardization(ISO) compartment arrange [1]), and for partner content with keys and use rules.
- License Server: This is network-side component gathers the data required to permit and allow license choice process, and encodes it.
- Secure agent: This component dwells on the end client side and is in charge of confirming the client identity, hardware integrity (against altering or tampering), and for getting, and decrypting permit grants from the license server.
- End user device: This device is specific for the CAS or DRM technology. It uses key sent by secure agent to implement content decryption

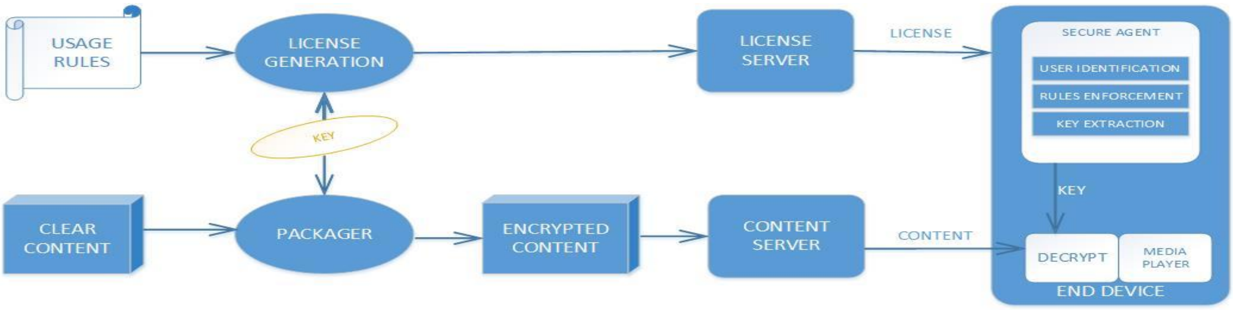
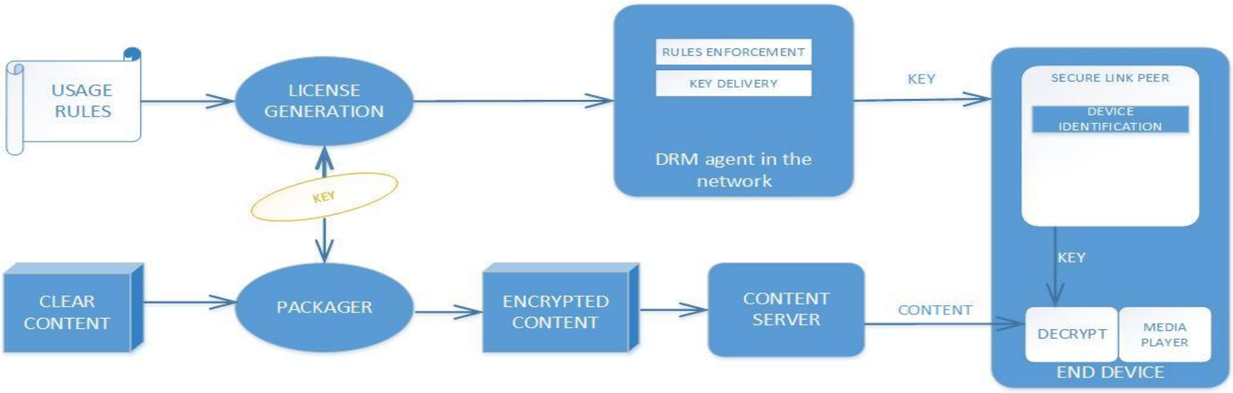


Figure: Un-Tethered model

Figure:Online DRM(Tethered model)



Online DRM:

The solution for the online DRM(Tethered Model) is moving the complete secure agent to the server side and the keys are obtained in a secure connection layer such as TLS (Transport Layer Security).

At the end device only thing is done here is identification of device which can be based on a certificate model, Keys are delivered by the server via secure layer which is immediately used to decrypt the content and deleted after the use. In case user requesting content is not legitimate the server denies the request.

III. Discussion

After studying both models in detail we analyzed the system advantages and flaws which are listed below:

Advantages of Un-Tethered Model:

- It provides [6] more versatility as various forms of DRM can be applied.

Flaws in Un-tethered system:

- Even though this model is versatile the main issue is secure agent lies on the end device hence[2] its easy for crackers to get the key or tamper with the rules enforced.

COMPARISION TABLE		
PARAMETER	**UN-TETHERED MODEL**	**TETHERED MODEL**
Security	Secure agent lies on the end device.	Secure agent lies on the server side.
License Management	Resides on the consumer's device.	Licenses are kept securely at external DRM centers offering centralized storage and security.
Access Management	Usually just requires a legit license then it doesn't enforce many restrictions.	Many restrictions are applied depending on the DRM service like Hardware bounded, limited time or usage, Number of simultaneous users, etc.
Payment Method	Usually offline, Digital copy is delivered in the form of CD or DVD, etc.	Usually online, Digital license is digitally delivered and content can be downloaded or used afterwards.
Application	Music CDs, Game DVDs.	General purpose.

Advantages in Tethered Model:

- Secure, since the vulnerability in un-tethered model has been moved to the server side.
- Flexible, same model can be used for almost any type of digital content.

Disadvantages in Tethered Model:

- Requires online authentication that means you need internet connection always.
- If license server is hacked or gets affected with the malware or Ddos attacked then this whole authentication fails.
- Requires high level security on the server side as any vulnerability may lead to leakage of license.

***Abbreviations*:**

DRM: Digital Rights Management.

ISO: International Organization for Standardization.

CAS: Conditional Access System.

TLS: Transport Layer Security.

DDOS: Distributed Denial of Service.

CD: Compact Disc.

DVD: Digital Versatile Disc.

IV. Conclusion

Both un-tethered and tethered model are used to restrict illegal access and redistribution of the digital content. But un-tethered model is comparatively easy to crack and tamper. The tethered model is better in terms of security as the authentication is done via an online server whenever the user wants to use the digital content. However, new tethered DRM techniques are only concerned about protecting interest of the content developers and hardly paying any attention towards consumer satisfaction as users are more annoyed by restrictions a tethered DRM poses such as Internet connectivity, not allowing users to access software or games unless they update to latest version, etc. Because of these dissatisfactions among consumer opens the new cause for a further research in this field.

V. References

1. International Organization for Standardization, “Information Technology—Coding of Audio-Visual Objects—Part 12: ISO Base Media File Format,” ISO/IEC 14496-12.

2. Farncombe Consulting Group, “Towards a Replacement for the DVB Common Scrambling Algorithm,” White Paper, Oct. 2009.
3. Liu, Q., Safavi-Naini, R., & Sheppard, N. P. (2003, January). Digital rights management for content distribution.In Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21 (pp. 49-58). Australian Computer Society, Inc..
4. Dong, Q., & Ji, P. Y. (2011, October). Research on Effect of Digital Entertainment in the Digital Era. In Knowledge Acquisition and Modeling (KAM), 2011 Fourth International Symposium on (pp. 566-567). IEEE.
5. Mampaey, M., & Villegas, Á. N. (2012). A Network-Centric DRM For Online Scenarios. Bell Labs Technical Journal, 17(3), 129-133.
6. Kwok, S. H. (2002). Digital rights management for the online music business. ACM Sigecom exchanges, 3(3), 17-24.Chicago.