An Analysis of BD+ and Other Major Schemes of DRM

Project members: Upendarreddy Mamidi (umamidi@gmu.edu)

Sangamitrareddy Katamreddy (skatamre@gmu.edu)

Urvi Tank (utank@gmu.edu)

Project Specification

Introduction:

Digital Rights Management (DRM) is a broad category of access control technologies that aims to restrict the use and copying of digital content on a wide range of devices. The idea is best explained as three terms: protection, copy prevention, and copy control. In reality, DRM is a program designed to prevent an individual without proper rights from copying or sharing a song, reading an ebook on another device, or playing a single-player game without an internet connection. The DRM schemes currently available are as follows:
Content Scrambling System (CSS): This type of DRM scheme is for traditional DVDs and is most commonly used by Toshiba and Matsushita. Due to its drawbacks there were many attacks on CSS.
Advanced Access Control System (AACS): This is DRM for next-gen video discs, such as HD, DVD, and Blu-Ray. Some Improvements over CSS were made in AACS. However, recently, many people are decrypting AACS.
BD+: This is a very advanced Protection. It was developed by Cryptography Research Inc. and is based on their Self-Protecting Digital Content concept. Its intent was to prevent unauthorized copies of Blu-ray discs and playback of Blu-ray media using unauthorized devices. It embeds a virtual machine in Blu-ray discs so that the discs will only play on authorized Blu-ray players.

Motivation: Our key motivation behind this project is to promote BD+ as the best and most advanced protection for the discs and as the key factor for victory of DVD war.

Goal of Investigation:

Mainly, our investigation aims to analyze various attacks on the CSS and AACS and the drawbacks of these schemes to better understand how such attacks occurred. We also aim to analyze the improvements made in the advanced protection and how BD+ improves security of Blu-ray.

HYPOTHESIS

BD+ is successful in securing the Blu-ray disc, and there are no vulnerabilities for attacks.

QUESTIONS

Is self-protecting Scheme reliable?
What is the functionality of self-protecting scheme?
What is the security mechanism of BD+?
Why is scrambling done before encryption and is the scrambling efficient?

Tentative Table of Contents:

1. Introduction.
2. Major Digital Rights Management schemes
3. Attacks over CSS and AACS
4. Overview and working of BD+
5. Future scope of improvements.
6. Conclusions
7. References

Timeline:

In the first phase (Oct. 15 to 17), we will study an overview of CSS and AACS, their respective attacks, and which improvements have been made in these schemes. In the second phase (Nov. 5 to 7), we will analyze overview of BD+ and the possible attacks against BD+. During the last phase (Nov. 19 to 21), we will be giving conclusion to hypothesis.

Resources:

[1] Jeremy Reimer (2007, o6, 17). “Blu-ray content protection agency certifies BD+” [Online]. Available: http://arstechnica.com/security/2007/06/blu-ray-content-protection-agency-certifies-bd/

[2] Wikipedia. “Advanced Access Content System” [online]. Available: http://en.wikipedia.org/wiki/Advanced_Access_Content_System

[3] Ryan Singel (2008, 02, 26). “How Crypto Won the DVD War” [online]. Available: http://www.wired.com/threatlevel/2008/02/how-crypto-won/