Team Members:

Anurag Kamat Haldonker and Jeremy Barthélemy

Title: **Encryption Schemes for Copy Protection of Digital Media**

Introduction & Motivation:

Software differs greatly from physical items in that software can be stolen, copied, and easily distributed to thousands of people, whereas physical objects cannot. For this reason, it lies in the best interests of owners of intellectual property to have security on their digital media. Unfortunately, there lies a serious and persistent problem with copyright protections with things such as video games, movies, software programs, and other forms of software.

Our goal is to research various encryption technologies currently used for copyright protection. We wish to discover the weaknesses and strengths of a variety of protection schemes, particularly HDCPv2, and also to look to the future in terms of what is needed to improve the security of intellectual properties.

Most importantly, we wish to look at various methods of software and hardware protection schemes (like watermarking and forensic reporting) and to see if and how the latest schemes implement these features. We also would like to gauge just how secure these schemes are by finding their possible vulnerabilities, their ability to adapt to these vulnerabilities, as well as their strengths.

In this paper we describe the 2nd version of interface independent adaptation of High-bandwidth Digital Content Protection (HDCP) system. The earlier version of the protocol HDCPv1 was used extensively in many devices starting around 2001 but in 2010 the master key of the protocol version was cracked which effectively made it an unsecure protocol to be used any further.

HDCPv2 overcomes a lot of limitations and flaws of the original protocol while maintaining its practicality. Although it is being used by a number of recently introduced devices, the new version of this protocol is yet to fully take off in the market. This project will provide us an opportunity to fully analyze the protocol and determine its advantages and disadvantages over the earlier version.

Alternative solutions (Protection Schemes to Explore):

HDCPv1.x (old version and it's problems)
HCDPv2
Explore steganographic procedures for watermarking algorithms

Problems to Investigate:

It is theoretically impossible to provide absolute copy protection. All forms of media will use something to play the intellectual media. The fact that the player needs to be able to read the media in order to present it to humans leads to the fact that a player can be built to read the media and make a copy of what is read. Is there any possible way to frustrate attempts to build such a player to copy from that which was read?

HDCPv1 has some limitations.

- It can work only with certain interfaces like DVI, HDMI, Display Port etc.
- It uses ad hoc 56-bit symmetric key system for authentication and encryption of data.
- It does not prevent a user from trying to proxy protected data to a remote device.
- Its master key has been cracked which means anyone can authenticate itself without a valid license.

Since HDCPv1 is no more useful for copy protection of digital content the industry requires a new protocol which can provide the same services as HDCPv1 and can remove certain flaws it has. HDCPv2 may be a better solution for preventing unauthorized copying of data. HDCPv2 is bound to have its own flaws, and we wish to investigate these flaws in detail.

Questions to be answered:

· How does HDCPv2 compare with its earlier version and other protocols? We wish to discuss the differences in how they perform with regard to algorithm, their weaknesses in a cryptanalysis sense, as well as their other general positive and negative attributes.

· Is the protocol competitive enough to make it into the devices being sold in the market?

· What are the advantages and drawbacks of this protocol?

· Vendors of digital media players generally are not provided much incentive to invest time and money in the implementation of superior software. How do we give them an incentive to develop better security for the owners of the intellectual media?

· How to allow for protection to grow and adapt as opposed to being static over the years?

· Is watermarking actually a feasible option for improving copy protection?

· What are the actual benefits of copy protection? Could it be possible that copy protection actually hinders the profits for many intellectual property owners? In other words, is it best to have minimal protection for some media and very strong protection in other forms of media?

· What are some other methods of performing forensic marking, particularly when the player is offline?

Verifying the results:

HDCPv2 uses RSA, AES and HMAC-SHA256 for encryption and also a certificate model with a revocation list for key management, all of which have been proven to be effectively implementable. Even the localization feature, which allows a HDCP transmitter to determine how far away a receiver is located, is implemented using a challenge question sent by the transmitter which needs to be answered correctly by the receiver within a short period of time. This version has been already chosen as the transport security for the wireless display standard MiraCast.

Milestones:

10/17/2012: Complete analysis of authentication and key exchange
10/31/2012: Complete analysis of HDCP encryption
11/14/2012: Complete analysis of Authentication Protocol Messages and Comparisons
11/28/2012: Prepare the final copy of the project report and presentation

Possible Modification of Specification:

If we find that there are other schemes that seem very likely to be widely implemented aside from HDCPv2, we may shift the focus to allow for more discussion of such schemes, along with comparison of the features of HDCPv2, or depending upon feedback for our report. We could also modify the specification if new revisions for HDCPv2 are released.

Table of contents:

References:

1. High-bandwidth Digital Content Protection System, Revision 2.1, July 18, 2011, http://www.digital-cp.com/files/static_page_files/DABB540C-1A4B-B294-D0008CB2D348FA19/HDCP%20Interface%20Independent%20Adaptation%20Specification%20Rev2_1.pdf
2. High-bandwidth Digital Content Protection System, Revision 1.4, July 8, 2009, http://www.digital-cp.com/files/static_page_files/DAD40C4C-1A4B-B294-D0E92C72CFE974A0/HDCP%20Specification%20Rev1_4_Secure.pdf
3. A Cryptanalysis of HDCPv2.1, Mathew Green, August 27, 2012, http://blog.cryptographyengineering.com/2012/08/reposted-cryptanalysis-of-hdcp-v2.html

4. A Copyright Protection using Watermarking Algorithm
   http://www.mii.lt/informatica/pdf/info631.pdf
5. Self-Protecting Digital Content
   http://www.cryptography.com/public/pdf/SelfProtectingContent.pdf
6. Old-School PC Copy Protection Schemes
   http://www.vintagecomputing.com/index.php/archives/174
7. DRM FAIL: Five Broken Copy Protection Schemes
   http://gigaom.com/video/drm-fail-five-broken-copy-protection-schemes-2/
8. Lessons from the Sony CD DRM Episode
   https://jhalderm.com/pub/papers/rootkit-sec06.pdf
9. CD/DVD/Media Protections
   http://www.cdmediaworld.com/hardware/cdrom/cd_protections.shtml
10. A Digital Image Copyright Protection Scheme Based on Visual Cryptography
    www2.tku.edu.tw/~tkjse/3-2/3-2-4.pdf
11. Copyright Protection Scheme for Digital Television Content
    International Journal of Information Technology, Vol. 11 No. 9 2005
12. Robust Signature-Based Copyright Protection Scheme Using the Most Significant Gray-Scale Bits of the Image
    www.hindawi.com/journals/am/2012/875759/