Digital Rights Management in Games

A Historical Survey

Patrick Austin, Amir Behmaram, Austin Smith, Eric Stutzman, Frances Vinlove – Team 1
University of Nevada, Reno, Department of Computer Science and Engineering
Reno, NV USA 89557

Abstract—**Digital rights management schemes have a long and inconsistent history in the entertainment software arena; many schemes have been tried, and almost all have failed, incurred significant costs to developers and legitimate users, or both. In this paper we offer a brief survey of the literature on software DRM, survey a number of historical DRM schemes, and offer a number of lessons for DRM implementation and avenues for further research drawn from our investigation.**

Keywords—digital rights management, software engineering, piracy, digital games

I. Introduction

Interactive entertainment has developed into a multibillion dollar industry over the past 50 years. For much of that period, developers of games have been embroiled in a costly arms race against software piracy. The field of digital rights management, or DRM, is concerned with attempts to restrict access to a piece of digital content to legitimate license holders only. In this paper we present a survey of the history of DRM in interactive entertainment, studying the literature of the subject and the record of historical and modern DRM successes and failures in order to offer lessons and recommendations for the field going forward.

The battle against piracy in the software space has cost software developers billions of dollars in research and development for DRM schemes and licensing fees for third-party DRM suites. DRM based on online authentication requires the costly maintenance of validation servers over the software's full lifetime. Failures of DRM security can and have led to widespread piracy; likewise, draconian DRM schemes run the risk of alienating even legitimate users, thereby deterring sales. Whether on the PC or on console platforms, software pirates in interactive entertainment have historically devised ingenious schemes to circumvent DRM nearly as quickly as DRM has been devised. To further compound the issue, it is difficult to accurately measure the impact of piracy on sales, considering that many each pirated software unit does not necessarily correspond to a lost sale.

Given that software DRM is a practical security problem with a long history and mixed success, we hope to draw out some interesting observations and lessons about best practices where a real-world engineering and security challenge meets real-world industry. We will discuss and draw lessons from a variety of tested and failed DRM schemes, from primitive early attempts to the far more sophisticated fare of the last 10-15 years. Common to all of these schemes are trade-offs between software performance, costs, convenience to legitimate users, and security. Of particular note to our investigation is the current reigning security scheme on the PC, a proprietary software security suite called Denuvo that has proved conspicuously durable against attacks since its introduction in late 2014.

II. Related Research

For this project several papers covering a variety of content were read and analyzed. Since the history of DRM is already covered in other sections of this paper, the following related work will focus on aspects of the interaction between consumers and the execution of DRM. These papers covered topics such as interesting approaches by the computer game industry to combat illegal game downloads to the acceptance of DRM systems by consumer markets.

Computer game piracy is an ongoing issue, but unlike the Recording Industry Association of America, Motion Picture Association of America and other entities, computer game developers and distributors avoid suing pirates or otherwise enforcing their rights through the legal system [1]. In lieu of this, the video-game industry has employed a variety of do-it-yourself remedies, such as digital rights management and online-only offerings, among others. As discussed in this paper, DRM has many issues, with the main issue being frustration from paying consumers when faced with the limitations a DRM-protected game includes.

Online-only offerings have been able to avoid the piracy problems that affect single-player games by hosting the game on an online server as opposed to an end-user's PC. The server handles the interaction between players, and the players see the results on their PC. Adding to the online-only offerings is the addition of a community surrounding the game, in which players can gain access to forums and in-game chats. Many games employing online-only offerings also have achievements, or "perks" that the player can collect after completing certain tasks, and display the perk badges on their profile. These two techniques mentioned coupled with the ease of downloading and installing the desired game quickly can be seen as tools for combating piracy.

Another strategy the video-game industry has come up with is online low-cost legal solutions, such as Steam and GOG, where players can buy games often at greatly reduced prices. The games are then downloaded and installed with just the click of a button, thus providing convenience and affordability for the user. This convenience and ease proves to be a deterrent for those users who might have illegally downloaded a copy of a game. These services also distribute patches and content updates for games hosted on the service, offering further user convenience that pirated copies cannot easily match.

One of the issues regarding piracy of video games is the lack of reliable data on the actual amount of games being pirated. A report from the Entertainment Software Association from December of 2009 claimed that over 9.78 million games were successfully downloaded illegally during that month. However, those figures only represented 200 games that were accessed on the most popular peer-to-peer (P2P) platforms like BitTorrent, eDonkey, Gnutella and Ares, while also neglecting to mention the legitimate sales figures for those same titles in that same month. [2].

There is currently no legally required system or measure in place for gathering data about sales and lost sales (for example, Steam does not release figures for games sold), and larger corporations do not respond to requests regarding their sales. This leads to at best skewed perceptions on the amount of pirated games and at worst incorrect and disproportionate figures, which does not contribute positively to solving the problem of piracy.

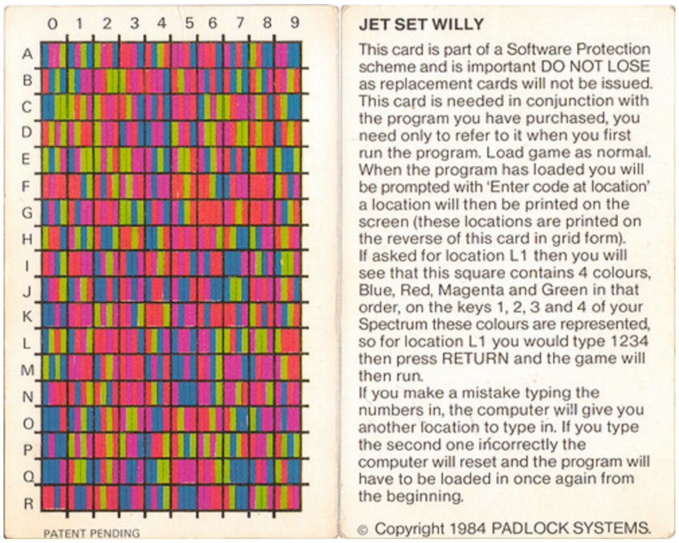
In order to further develop strategies to reduce piracy of games, solid data regarding pirated copies needs to be collected and analyzed in order to approach the issue efficiently. Cooperation between mainstream companies and consumers will lead to a better understanding of the world of piracy and a corresponding reduction in the amount of piracy.

III. METHODS

Research was the primary method used to accomplish our goals. Initially, we completed a thorough survey of the Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM) online libraries. Then we used OneSearch, the UNR Online Research Library, to find other journal articles pertaining to DRM. This guided the direction of our paper, ensuring that we approached DRM schemes with a realistic perspective. Finally, we used security forums and recent news reports concerning DRM to inform our final conclusion on how DRM schemes are being circumvented and what the future may hold for these algorithms.

IV. RESULTS AND ANALYSIS

The earlier methods of DRM from the late 80's to early 90's were simple and mainly required physical objects such as code wheels, dongles, text from the game manual, or code books as seen in Fig. 1. These earlier methods didn't need to be too complex mainly because the copying and redistribution of games for free at the time wasn't nearly as prevalent as today, primarily due to the lack of the technology required to do so on a large scale. These schemes live on as a topic of curiosity and frustration in the modern day, as the destruction and loss of analog media like instruction manuals over time can make overcoming the DRM to play these games in the modern day a challenge.



JET SET WILLY

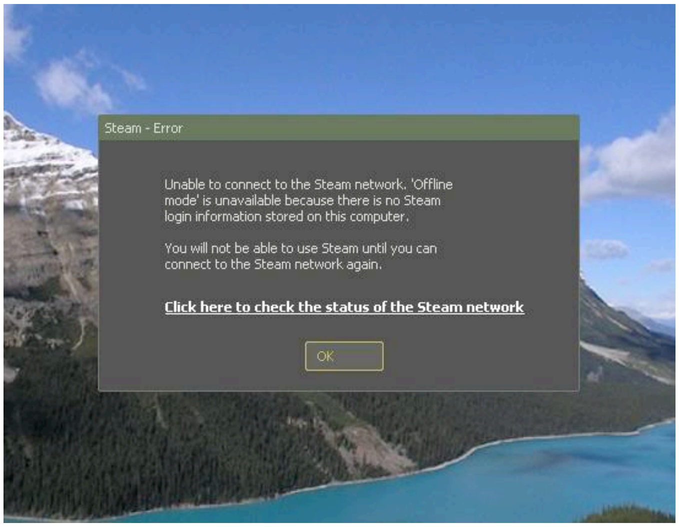
This card is part of a Software Protection scheme and is important DO NOT LOSE as replacement cards will not be issued. This card is needed in conjunction with the program you have purchased, you need only to refer to it when you first run the program. Load game as normal. When the program has loaded you will be prompted with 'Enter code at location' a location will then be printed on the screen (these locations are printed on the reverse of this card in grid form). If asked for location L1 then you will see that this square contains 4 colours, Blue, Red, Magenta and Green in that order, on the keys 1, 2, 3 and 4 of your Spectrum these colours are represented, so for location L1 you would type 1234 then press RETURN and the game will then run. If you make a mistake typing the numbers in, the computer will give you another location to type in. If you type the second one incorrectly the computer will reset and the program will have to be loaded in once again from the beginning.

© Copyright 1984 PADLOCK SYSTEMS.

Figure 1. A photograph of the Jet Set Willy instruction manual from 1984

Later, as new technology became available circa the late 90's to mid 2000's newer forms of DRM such as serial numbers and keys, online distributors, and constant internet connection DRM became more popular ways to combat piracy, as seen below in Fig. 2. While these methods were in fact a step up in terms of security from earlier methods they still had their problems. Serial numbers and keys were most common with CD's and had the codes printed on the package. These keys often didn't prevent copying and could be used multiple times; unique CD key schemes could compromise legitimate user keys if the key generation scheme was overcome by pirates [3].

Online distribution left the DRM up to the hosting service and prevented the games from being resold. Constant internet connection is a problem especially with single player games which normally don't require players to be online. The cost of maintaining these servers over a game's lifetime, or in perpetuity, can cease to be cost effective. For that reason, a growing number of games originally requiring online-only DRM have effectively vanished forever, never to be experienced again, with the shutdown of online authentication servers that were required to play the game at all.



Unable to connect to the Steam network. 'Offline mode' is unavailable because there is no Steam login information stored on this computer.

You will not be able to use Steam until you can connect to the Steam network again.

Click here to check the status of the Steam network

Figure 2. Screenshot of Steam connection error

The latest DRM method is Denuvo, a proprietary software suite. This software is complex and expensive. The software is licensed to developers in a package and it is left up to them to integrate the DRM into the game executable. This requirement means the security of the DRM is largely up to the developers and how they go about integrating it into the code of the game. This is the reason why some games that have used this software haven't been cracked in weeks or months, while others have been cracked within days. However, given the high price tag of this software, it is usually only implemented in AAA games with large budgets. These games sell a majority of their games in the first few weeks of release in a model similar to that experienced by the film industry. Denuvo is meant to be used as more of a front-loaded DRM to prevent piracy within this launch window, protecting the period of greatest revenue gain, rather than a form of DRM expected to stand in perpetuity. In this respect, Denuvo can claim success even in cases where it is eventually circumvented.

V. CONCLUSION

After researching the topic thoroughly, we conclude that current DRM practices in the video game industry have a negative impact on developers, distributors, and users. In Table 1 we compare and discuss advantages and disadvantages of various DRM schemes that have been used over the past several decades [4]. No matter how developers and distributors try to implement DRM methods to their content, the success rate of such security schemes in most cases is poor, especially in the long term but often even in the short term. Even if software developers implement an expensive method like Denuvo into their games, the game is still likely to be pirated. This is obviously a financial hit to developers and distributors as they are losing out on sales. Whether it's the download sizes that are growing in size, or methods used by distributors like serial keys and limiting the download to a fixed number of systems, legitimate users are also often negatively impacted by DRM schemes.

This has led us to propose several suggestions to improve current DRM methods. If possible, DRM-free software is often a preferable solution for all parties, and has been attempted with significant success by the digital storefront Good Old Games. Users won't experience the negative side effects of DRM, developers won't have to deal licensing costs and development time lost implementing the methods such as Denuvo into their code, and distributors won't have to face the costs of DRM implementation and DRM failure. If completely getting rid of DRM isn't an option, then focusing on the front-end method of DRM to cover the launch window of expensive, yearly games (titles like Call of Duty, Battlefield, etc.), whose user base usually switch from game to game, may be a necessary evil. For games that are more likely to be around for longer periods of time, always online DRM would be the best option, though historians of games have reason to be concerned that these games might vanish forever when their servers cease to be economical to maintain. Whatever the change may be, we feel that there needs to be one, as current methods are frequently far from ideal for both users and developers.

Table 1. Advantages and Disadvantages of Various DRM Schemes

Types of DRM	Description	Advantages	Disadvantages
On-disk copy protection (Key disks)	Used with floppy discs, techniques were applied to determine if the floppy disc was an original one or not. This was accomplished by intentionally modifying, odd address marks, different track layout, and file encryption.	Hard to replicate the protection schemes placed onto the floppy discs.	Floppy Disks are incredibly flimsy, so if your copy broke you would have to buy a new version of the game.
Manual Lookup	This method requires you to look up a specific code that was given to you once the game was purchased. You would then have to enter this code at some point while playing the game in order to continue playing.	Completely protected the game if the user did not have a code.	Sometimes these codes were annoying to enter. Also, most of these codes could be shared / photocopied.
The code wheel	When purchasing a game, you were given a code wheel which needed to be used to in order to beat certain levels of the game.	These code wheels were integrated with game levels, making them feel less meticulous than a manual lookup.	Code wheels could still be photocopied and distributed if you had the right resources.
Unique physical locks	Tangible items that were shipped with a game that needed to be used to decipher different codes within the game or game manual.	These codes would be impossible to figure out without the physical lock.	The physical items were not always of the highest quality and could break. Since they were a physical item, if you were to lose the item you would be locked out of your game.
Serial Number and Keys	Used mostly with CD's. A unique key code was printed somewhere within the user manual or package, and needed to be entered before installing the CD.	Could not install a CD game without the unique code, and was a relatively easy process for the user.	It did a poor job at preventing copying as the unique code could be used multiple times.
3rd-Party DRM (Safedisc, Securom, Starforce)	Prevent copying by applying digital signatures or electronic fingerprints to a disc during mastering and assigned a unique number to the disc.	Made it very difficult to crack a game at first. For example, Splinter Cell took 422 days before it was cracked.	These 3rd party DRM's sometimes acted like malware, and bloated you computer. They also installed hard to remove device drivers causing system instability.
Online Distribution	Retail services combined with DRM. Sold by the client and verified by the servers. These can usually just run in the background while playing the game. Examples of these include Steam, Games for Windows Live, Origin, and Uplay.	Made it easy for game developers to have DRM on their games by leaving it up to the hosting service.	Can sometimes be Sub-Par due to crappy user interfaces, inconsistent logins, and poorly used patching systems. Can't resell any of your games, and usually have to be played online.
Online Activation	Accomplished by entering a serial number into the game which can then be verified online.	Without a serial number it was nearly impossible to play the game.	These would sometimes limit the amount of installations you could use per game.
Constant Internet Connection DRM	DRM that is always online, always connected, and always making sure that your account is authenticated.	It is constantly running checks in the background to verify that you are using a legit copy of the game.	If you lost connection while playing then you could not play your game. Also could cause lag if you had a poor internet connection.

VI. FUTURE RESEARCH WORK DIRECTIONS

DRM continues to be a pivotal component when releasing video games to the populace. As computing power becomes more and more powerful, DRM will need to continue to make progress as well. As these new technologies become presented to the public, DRM engineers must learn from past mistakes in order to create protection schemes that will endure the test of time. Once these new technologies are introduced, it is recommended that researchers continue to analyze the pros and cons of new DRM's. Once analyzed, they can learn from previous attempts at DRM, and continue to make positive advancements.

If DRM is to continue being a part of the video game industry then there are a couple of options that seem to be the most logical for developers to pursue. There is a robust cryptographic theory that has been applied to the problem of delivering digital content, yet this is no comparable method for DRM [5]. Implementing this method with DRM would help test any methods for vulnerabilities and produce stronger DRM methods. If the DRM is to be implemented on a AAA title then the use of front-loaded DRM would make the most sense, primarily to prevent piracy within the launch window of the first several weeks. If the game is going to be a long-standing game which will have active users for many years an always online DRM option might be the most effective.

Another possibility would be to attempt to strengthen the DRM techniques themselves. Currently all commonly used DRM is proprietary which means it doesn't have the luxury of being tested and analyzed at by others for any weaknesses [6]. It seems that making DRM open source or at least having some kind of analysis of the implementation to look for weaknesses would be one of the next logical steps to take in order maintain the strength of any DRM system. The proposed strategy would be similar to Cryptanalysis in the field of Cryptography in which the implementation is analyzed and tested by experts to determine if there are any vulnerabilities. Some developers, like Nintendo, have also begun to experiment with bounty systems which pay for the disclosure of security vulnerabilities; we recommend further experimentation with this approach.

The final option would be to go DRM-free entirely. Some video game distributors such as gog.com have managed to go fully DRM-free with considerable success. Given the checkered history of DRM, its inclusion may actually serve as a deterrent to some users as it makes the file download bigger and may even lead to slower performance of the game. We feel that these options would be the most effective in combatting piracy and strengthening current DRM methods.

REFERENCES

[1] P. Holm, "Piracy on the simulated seas: the computer games industry's non-legal approaches to fighting illegal downloads of games", Stanford Law School, Information & Communications Technology Law, Vol. 23, No. 1, 2014.

[2] Tamsin Oxford, 2017, "The truth about PC game piracy", TechRadar, http://www.techradar.com/news/gaming/the-truth-about-pc-game-piracy-688864.

[3] R. Hyams, "Copy Protection Of Computer Games", Department of Mathematics, University of London, 1st ed. Royal Holloway, 2008.

[4] T. Hauser, C. Wenz, "DRM Under Attack: Weaknesses in Existing Systems", Digital Rights Management-Technological, Economic, Legal and Political Aspects, pp 206-223, 2003.

[5] M. Stamp, "Digital Rights Management: The Technology Behind The Hype", San Jose State University, Journal of Electronic Commerce Research, Vol. 4, No. 3, pp. 102-112, 2003.

[6] H.L. Jonker, S. Mauw, J.H.S. Verschuren, and A.T.S.C. Schoonen. "Security aspects of DRM systems", 25th Symposium on Information Theory in the Benelux, pp. 169-176, 2004.