Video Game DRM: Analysis and Paradigm Solution

Karthik J, Amritha P P, and Sethumadhavan M

TIFAC-CORE in Cyber Security
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham, India

karthik9497@outlook.com, {pp_amritha, m_sethu}@cb.amrita.edu

***Abstract*—Video game piracy is the illegal downloading and sharing of video game content, a type of copyright infringement. It is a major problem faced by video game publishers when selling their games, owing to the ease of downloading games through torrents or DDL websites. Digital Rights Management (DRM) tools are used to hinder piracy. And yet DRM remains a false barrier as crackers invariably break the DRM and release the video game on P2P file sharing platforms and torrent websites within few days of the launch of the video game. This research paper investigates the existing DRM or copy protection methods used in video games and presents new solutions that could be implemented with DRM thereby making the video games harder to crack.**

Keywords—Digital Rights Management (DRM), video game, piracy, copy protection, Denuvo

I. INTRODUCTION

Digital Rights Management (DRM) or copy protection for video games are a set of measures to protect the games from being copied freely. From the dawn of video games, the usage of copy protection has been prevalent.

It was not until the widespread use of floppy disks in the late seventies and early eighties that a truly effective copy protection scheme came about: On-disk copy protection. Floppy disks work by attaching magnetic values to a spinning piece of metal coated plastic. During the manufacturing process, certain techniques like intentionally bad sectors, odd address marks, different track layouts, file encryption, etc. can be applied to let the software know if it's an original disk being used. Using this technique, the game could not be installed to the hard disk and the players could not take personal backups of their disks. The floppy disks are fragile, and they easily got bent out of shape. They are susceptible to magnetic fields, heat, and dirt. This led to gamers becoming frustrated as they had to buy the game again if something happened to it.

The most common method of copy protection amongst games of the mid to late 80's was manual lookup or passphrase also known as Off-disk copy protection. This method involves the game telling you to look up a random phrase/code in the manual provided with the game at some point. The weakness of this protection being that the phrase/code is not unique.

It wasn't long before other methods were used to verify CD-ROM games like Serial numbers and Alphanumeric keys. The game got a unique key code often printed in the manual which the user must input in order to complete the installation. If activation is completed offline, then a single key has unlimited uses. If key activation is completed online, then a single key may be limited to a specific number of installations. It did not prevent much copying as within a few weeks, crackers are able to retool a working key generator for the game. So, of course more protection was deemed necessary, and manufactures moved on to what is most thought out today as DRM.

Third-party systems like SafeDisc, SecuROM, and StarForce attempted to prevent copying by applying digital signatures or electronic fingerprints to a disk during mastering and assigns a unique number to the disk [1]. There were claims that these DRM works like malware in that it degrades optical drive performance with continued use. Also, the software and device drivers it underhandedly installs was hard to remove and acts as somewhat of a rootkit and caused all manner of system instability.

There are a few examples of slightly more creative DRM methods like FADE. It is a system which was used in FPS games like Operation Flashpoint and Arma II where the gameplay will gradually get worse and worse if a pirated copy is detected. Eventually getting to the point where you could not aim your gun or walk straight.

Another very common way of providing DRM service is online distribution like Steam, Games for Windows Live, Origin and Uplay. These are retail services among other things that are combined with DRM. Games sold through these digital distribution platforms tend to have stacked DRM protection i.e. they use third party DRMs like Denuvo, VMProtect along with their own DRM. Games are sold via the client verified via servers and the client runs in the background during gameplay. These DRMs are easily cracked by the warez scene in a matter of days following the game's release.

And lastly, we have what is probably the least liked of all DRM systems thus far: constant internet-connected DRM. This is DRM that is always online, always connected. Gamers had to have a reliable broadband connection and an outstanding router, not to mention hoping that the company's authentication servers are online, because if anything goes wrong, then they could not

play the game they paid money for. Ubisoft's Assassin's Creed II was notorious for this when it first launched, it wasn't uncommon to find the servers down for several days at a time. No one could log in to play the single player game and if connection was lost while playing, the players lost the progress of the game back to the last checkpoint [2]. Not only that but sometimes the connection was not that great, and gamers were ended up with lag in a single player game. But games using this DRM are impossible to crack as long as the game connects to the developer's servers.

In this paper, we analyze the DRM protection methods and propose DRM measures which could be implemented alongside the DRM technologies to make the video games difficult to crack.

II. Related Work

As DRM vendors like Denuvo, VMProtect, Arxan need to be secretive about their DRM implementations, they do not disclose information about their DRM software. So, there are not much research conducted in this area. However, there have been research conducted about the scene groups that crack the DRM software. It focuses on the aspect of pirated video games being an ideal vector for distribution of malware [4].

Another research paper explains StarForce DRM software as case study and proposes that the protection failed as it caused computer instability and crashes the user system [1].

Work done by Adam Kozakiewicz and Krzysztof Lasota conveys that Always-Online DRM cannot be the perfect solution as customers will be left with no way to play the game they bought after the company decides to pull the plug on their servers [6].

The methods that can be used to reinforce video game DRM and the performance impact of games with Denuvo DRM is not present in the previous works and is presented in this paper.

III. Game Piracy

Game Piracy has been a contentious issue in the PC community. Video games cost a huge amount of money to develop and it must be protected. The game developers stacked DRM upon DRM to minimize piracy. But the warez groups which comprises of teams of individuals skilled in reverse engineering and cracking the DRM measures applied to the video game usually crack and release copies of games within few days after the launch of the video game [3]. These pirate groups can be classified by the role they play in production and distribution of these cracks.

A. Warez Scene

The warez scene groups are known for their consistent, reliable, and secure cracks. They are restricted in their methods used to crack game protections. If a group uses a disallowed method, the crack is nuked i.e. other scene groups flag the crack as inappropriate. The releases that are nuked by the scene groups is often followed by a proper crack that fixes the issues which plagued the nuked release. The warez scene is a cornerstone of game piracy and as such has been subject to numerous raids by law-enforcement agencies around the world. Unsurprisingly, these scene groups tend to be secretive and do not speak to the press or the public instead they communicate through their nfo files they bundle along with their cracks. These nfo files are distinguished by the decorative ASCII artstyle. These scene groups do not host websites and do not seek a profit. They rarely if ever make a penny from their releases but they do it for the thrill of beating other groups at cracking new protections.

B. P2P Groups

All non-scene groups can be classified as Peer-to-peer groups. They are not bound by scene standards and restrictions, thereby having many methods at their disposal to break DRMs. This was evident when Revolt's Voksi used a kernel driver to bypass Denuvo's protection, a method which is off-limits to the warez scene. By using the large number of techniques available to them, they often beat the scene and produce the first cracks. But the quality of peer-to-peer cracks is often dubious and nowhere near the cracks by the scene groups.

C. Repackers

Repackers do not crack the games themselves like the two previous groups but rather they compress those releases by scene and P2P groups down to smaller sizes. These compressed files are then bundled with customized installers and are distributed in what is called as repacks. These repacks isolates language files so only the language needed can be installed further saving hard drive space. These releases pose the greatest risk as they have been reported to contain malware. This was perceptible when Just Cause 3 and Rise of the Tomb Raider repacks were bundled with Bitcoin miners that silently carried out mining operations without the user's consent [4].

IV. Analysis of Video Game DRM

Gamers have been dealing with intrusive DRMs like SecuROM, StarForce, Arxan, and more recently Denuvo all for the sake of delaying piracy. However, these DRM protections have only managed to delay piracy and none of them have ever completely prevented a cracked release. The only one that has managed to achieve that feat is by far the most intrusive, restrictive - always-online DRM. Always-online DRM is not an additional layer of protection added to the game post development like Denuvo but rather a restriction built into the games designed by the developers. Some might call Denuvo an always-on DRM as it has been reported to deny buyers access to their games when their connection goes down. Always-on DRM has existed on a spectrum of game design practices like periodic activation, continuous authentication.

A. Periodic Activation

Denuvo appears to be using periodic activation as one of its many measures as evidenced by the fact that buyers need to log in every few days to authenticate their games [5]. However, when the Denuvo's activation servers fail, it ruins the experience for legit customers. This happened when Denuvo's servers prevented legitimate buyers from playing Batman Arkham Knight as they couldn't reach the authentication server to activate their legitimate copies. Pirates meanwhile were unaffected by the outages as the game was cracked at that point by a scene group that has managed to emulate these activations offline with their cracks. Nevertheless, this outage provides a glimpse of what is to come when Denuvo's servers shut down

for good as buyers will have no way to play the games they paid for if no crack is available for the games in question.

B. *Continuous Authentication*

Games that require continuous authentication will kick you out mid-session if your internet connection goes down and how long it will take for the game to disconnect depends on the implementation used and varies from game to game. For instance, Assassin's Creed 2 stops five seconds after disconnection. The game companies often justify implementing this draconian measure by insisting their game is better off for its online services but the excuses never hold up. For instance, the developers of 2015's Need for Speed insisted their game needed to be online as it was a social experience. Nevertheless we fail to see why this precluded the ability to play offline as previous Need for Speed titles have had robust multiplayer without imposing always online requirements. This seems like a thinly veiled excuse to disguise this intrusive DRM as a legitimate requirement for a critical game feature. The DRM itself has been highly successful in this case as Need for Speed is yet to be cracked and probably will never be. But once the company decides to pull the plug on their servers, there is no way to play the game for customers who bought the legit copy [6].

While these methods does stop pirates from playing the game, it eventually but inevitably does the same to buyers who paid for the game. Always-online DRM has already rendered several games permanently unplayable which is the fate destined for any game that requires a persistent connection.

V. Performance Analysis of Denuvo DRM

The purpose of DRM is to keep the game safe from piracy during the initial sales window. So, once the scene groups crack the game, the developers of the game sometimes tend to remove the anti-tamper DRM from the game [7]. We compare both releases (with and without DRM) of three games using the benchmarks displayed in table 2 to find out whether the DRM has an impact on the game's performance.

The specifications of the PC used for running the analysis is shown in table 1. While performing the analysis, identical graphics settings are used for both runs of the game.

TABLE I. PC Specifications

Part	Description
CPU	Intel Core i7-7700HQ @2.80 GHZ
GPU	Nvidia GeForce GTX 1060 (6GB DDR5)
RAM	16 GB DDR4

TABLE II. Benchmarks used for Testing

Benchmarks	Unit
Frame rate (The higher the better)	FPS
Loading time (The lower the better)	seconds
.exe file size (The lower the better)	MB

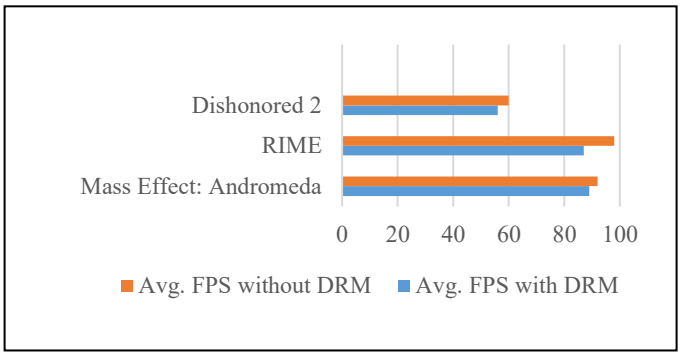

Fig. 1. Frame Rate Benchmark

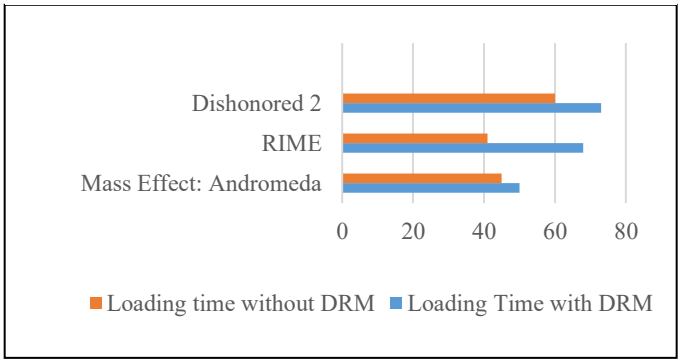

Fig. 2. Loading Time Benchmark

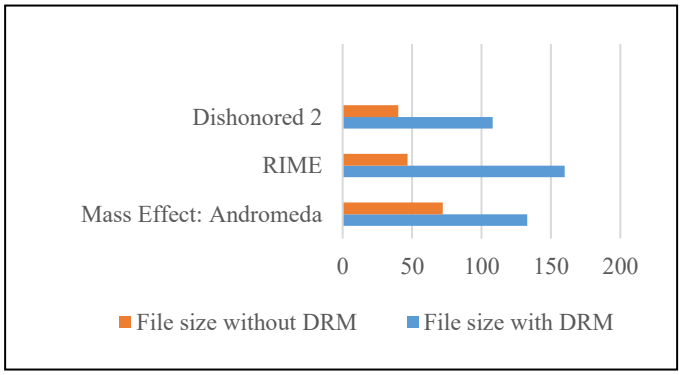

Fig. 3. File Size Comparison

The results in Fig. 1, 2, and 3 shows that there was an average of 8% increase in FPS, 32% decrease in loading time, and 60% decrease in .exe file size across the games with no DRM in comparison with the respective DRM-enabled run. This shows that DRM technologies have a huge impact on the performance of the video game. This will be more evident in case of low PC configuration systems.

VI. Proposed Solution

A. Offloaded Server-side code

This method works by delivering an incomplete game to the customers that relies on the developer's servers for crucial gameplay functions. It can be achieved by offloading certain parts of the game to a server which the game then requests at runtime. By this method, the cracked version will be unable to access features of the game that require an internet connection, as the code for that content is stored on the developer's servers. Also, the scene cannot release an incomplete game as any cracked release should be identical to the legitimate version. It can only be observed and imitated at best and the backend code can be mimicked using server emulators, but this will not match the legitimate experience to the degree required by scene standards.

B. On-the-fly Encryption

The common method of video game cracking is removing the DRM checks in the exe file by reverse engineering and modifying the file of the video game so that in the cracked version no DRM checks are present, and anyone can play the game without buying. This can be overcome by following the underlying measures. When the user installs a game from a digital distribution platform, the game files need to be encrypted on the fly using the encrypting file system feature of OS like EFS found in Windows 10 Pro, and Enterprise versions. Once encrypted, the game files must not be accessible for modification even if full access permissions are granted thereby making it impossible for crackers to reverse engineer and remove the DRM checks. All the decryption operations are done on the Trusted Execution Environment (TEE) and then loaded into memory. Thus, the game files are protected which will lead to difficulties in modifying the game.

C. Game Launch Limitation

The games must be made launchable only via the client application of the digital distribution platform and not via Explorer or CMD Prompt By following this method, only the authenticated users of the digital distribution platform like Steam, Epic Games can play the game as there is a prerequisite that the user must first launch the client.

D. Scattered DRM checks

The DRM measures must not be directly built into the exe but instead scattered around in DLL files. In the existing methods, the DRM checks are present only in the .exe file of the game. By deploying the DRM checks not only in .exe file but also in game critical DLL files, it will harder for crackers to circumvent the DRM.

A brief summary of the proposed DRM measures is shown in the figure 4.

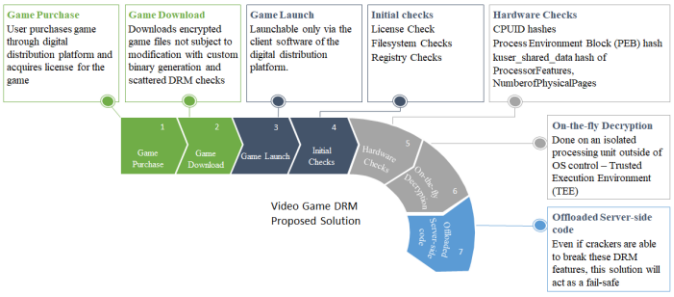

Fig. 4. Proposed Solution Overview

VII. Conclusion

In this paper, we have analyzed the existing DRM technologies and found out they are easily susceptible to cracking and the only method that offers some protection is always-online DRM. We conclude that always-online DRM succeeds in rendering games unusable first for pirates and later for legitimate buyers as well. The length of time customers gets to use the product they're paid for is entirely at the company's discretion. On running the benchmark tests for games before and after removal of Denuvo DRM protection, we also found that the DRM software had a significant impact on the performance of the video games. We have proposed four DRM measures that could go a long way in making the game tougher to crack. As future work, in the proposed On-the-fly encryption method, decrypting the game in real time using very low CPU resources without much compromise on game performance could be done.

References

[1] D. Chaboya, "State of the Practice of Software Anti-Tamper," Air Force Research Labs Wright Patterson AFB United States, 2007.

[2] B. Kuchera, "Official explanation of controversial Assassin's Creed 2 DRM." Escapist Magazine, http://arstechnica.com/gaming/2010/02/ubisoft-details-drm. ars. Retrieved. pp. 03-27, 2010.

[3] C. Cortner, "The Warez Scene," 2008.

[4] A.V. Moshirnia, "Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat," Ind. LJ, 93, p. 975, 2018.

[5] R. M. Parizi, A. Dehghantanha, K. K. R. Choo, M. Hammoudeh, and G. Epiphaniou, "Security in online games: Current implementations and challenges," Handbook of Big Data and IoT Security, Springer, Cham, pp. 367-384, 2019.

[6] A. Kozakiewicz and K. Lasota, "Secure DRM mechanism for offline applications," 2015 International Conference on Military Communications and Information Systems (ICMCIS), Cracow, pp. 1-8, 2015.

[7] N. Grayson, "Denuvo Says Doom Dropped Their Anti-Piracy Tech Because It Got The Job Done," 2016.