Proceedings of the 2nd International Conference on Functional Materials and Civil Engineering
DOI: 10.54254/2755-2721/89/20241059

Cryptography and DRM: A study of digital copyright protection in the gaming industry

Liwen Zhang

Department of Computer Science and Physics, University of California, UC Davis, America

1300133435@qq.com

Abstract. This paper explores the role of cryptography and encryption technology in the evolution of digital rights management (DRM) in the gaming industry. A collection of guidelines, procedures, and instruments that control the appropriate use of digital content is collectively referred to as digital rights management (DRM). Cryptography plays a vital role in DRM by ensuring data privacy, authenticity, and integrity. The early stages of DRM in gaming involved physical disc-based methods, such as unique disc features and online activation. However, these methods faced challenges such as compatibility issues and unauthorized copying. Modern DRM techniques incorporate advanced cryptographic techniques and account-based DRM tied to user accounts. Cryptography in DRM secures the distribution and consumption of digital content by converting game data into an unreadable format, which can only be decrypted with a valid key. The paper also discusses the use of third-party DRM technologies like Denuvo, which employ robust encryption and obfuscation methods. However, third-party DRM can have performance impacts, inconvenience users, and lead to compatibility issues. The paper emphasizes the need for continuous refinement of DRM technologies to balance copyright protection and consumer rights in the evolving gaming industry.

Keywords: DRM, cryptography, Gaming Industry, third-party DRM technologies.

1. Introduction

In today's digital age, the gaming industry faces a myriad of challenges and opportunities. Foremost among these challenges is protecting creators' rights against rampant unauthorized copying and distribution. Cryptography and Digital Rights Management (DRM) emerge as pivotal solutions. Cryptography converts readable data into an unreadable format using mathematical algorithms, ensuring data privacy and integrity. Integral to this is DRM, a strategy employed to protect digital media copyright. This approach, dependent on cryptography, controls how consumers interact with their purchased digital content. Though DRM spans various media, its role within the gaming industry, especially given the industry's shift towards digital distribution, is the focus of this paper. The implementation of DRM in gaming has seen various milestones and controversies, such as its use in games like 'Mass Effect' and 'Spore'. These particular DRM methods were met with significant public outcry and even resulted in heightened piracy rates. This paper seeks to delve deep into the intricate relationship between cryptography and the evolution of DRM in gaming. We'll analyze the trajectory

DOI: 10.54254/2755-2721/89/20241059

of these technologies, their influence on DRM mechanisms, and their current implications. Furthermore, we'll touch upon the crucial balance the industry needs to strike between safeguarding intellectual property and respecting consumer rights [1].

2. Evolution and Implications of Game DRM: From Disc-Based Protections to Modern Challenges

2.1. Early Stage

In the nascent years of gaming, when optical discs were the standard medium, the security measures in place had a distinctly physical nature. Games leveraged the tangible characteristics of discs to combat piracy. This took the form of incorporating special physical features on the disc, such as intentional errors or unique patterns. The uniqueness of these features made unauthorized replication a daunting task.

One common DRM technique involved incorporating special physical features on the disc, such as intentional errors or unique patterns. These features were difficult to replicate accurately, making it challenging to create functional copies of the original disc. The game's program or resource files were often encrypted or encoded in a way that required the presence of these physical features for successful decryption. However, this technique has compatibility and disc damage problems. Because the presence of special physical features on the disc could cause compatibility problems with certain disc drives or players. Some users might experience difficulties in reading or running the game due to compatibility issues. Besides, Intentional errors or unique patterns on the disc could make it more susceptible to damage. Even minor scratches or wear on the disc could render it unreadable or cause errors during the decryption process, preventing legitimate users from accessing the game.

Additionally, disc-based DRM systems often required users to have the original disc inserted into their computer's optical drive while playing the game. This was done to verify the authenticity of the disc and ensure that it hadn't been duplicated or illegally distributed. The game would check for specific indicators on the disc, such as hidden sectors or unique identifiers, to validate its legitimacy. Despite the DRM measures in place, determined individuals could find ways to bypass the disc-based authentication system and create unauthorized copies of the game.

Some games also employed additional measures like online activation or verification processes, where users had to enter unique serial numbers or connect to a server to authenticate their copy of the game. These methods helped prevent unauthorized use of the software and protected the rights of game developers and publishers. However, it did not prevent copying as within a few weeks, crackers are able to retool a working key generator for the game. Due to the various issues mentioned earlier, games required additional protection, leading manufacturers to turn to what is now considered the modern DRM research.

2.2. Modern DRM Technology

In response to the glaring limitations of disc-based protections, the digital age ushered in a more sophisticated DRM technology. Central to this shift was the adoption of 128-bit AES encryption. Renowned for its resilience against breaches, this encryption ensured that even if a rogue element got their hands on the game file, they'd be left with an indecipherable puzzle [2].

For DRM to function, users must possess media players that can recognize protected content and request the corresponding key to unlock it. Additionally, rights holders must operate a license server that responds to legitimate requests by providing the key required to reverse the encryption [3].

Considering offline DRM technology, it will be continuously scrutinized and exploited by warez groups, resulting in the development of replicas. Modern DRM technologies, for the most part, require network authentication. A very common way of providing modern DRM service is online distribution like Steam, Games for Windows Live, Origin and Uplay [4]. They act as both retail services and DRM solutions. They provide a centralized marketplace where users can purchase and download games securely. These platforms require users to create accounts and install client software, which serves as a

DOI: 10.54254/2755-2721/89/20241059

gateway to access and manage their game library. They 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 [5].

2.3. Third-party DRM problems

Denuvo stands out in the modern DRM landscape, garnering attention for its potent blend of encryption and obfuscation. Yet, beneath its cryptic exterior, Denuvo's mechanisms are intricate. It creates a virtual environment, securely sealed, within which the game's code breathes. Coupled with this is Denuvo's penchant for code obfuscation, making any hacker's attempt at deciphering it akin to navigating a labyrinth blindfolded.

A significant element of Denuvo's approach is the use of a virtual machine, which executes the game's code within a highly protected virtual environment. This virtual machine is heavily obfuscated, employing multiple layers of encryption and anti-debugging measures to deter hackers from analyzing or manipulating the code [6].

In addition to the virtual machine, Denuvo employs various other obfuscation techniques like code splitting, making it challenging for hackers to comprehend the structure and flow of the game's code. It also incorporates anti-debugging measures such as memory scrambling to thwart attempts by hackers to attach debuggers and examine the game's behavior [7].

Although third-party DRM like Denuvo is considered one of the most effective anti-tampering solutions available, it does have some problems.

Performance Impact: third-party DRM, including Denuvo, can introduce performance overhead to games. Users have reported decreased frame rates and longer loading times when DRM is present, which can negatively impact the gaming experience. Such as, Resident Evil Village [8].

Inconvenience: Several players have voiced concerns about the inability to launch Denuvo-protected games in the absence of an internet connection. The stringent online verification system employed by Denuvo necessitates a connection to its servers at game startup to confirm its authenticity. This system impediment can hamper those who predominantly rely on offline gaming or are in areas with sporadic internet access. Taking "Assassin’s Creed II" and "Diablo III" as case studies, these games exemplify a growing trend where even single-player modes necessitate online connectivity. These design decisions by developers mean that players without a consistent internet connection, or those who often switch to offline modes, are left at a disadvantage, making the gaming experience less inclusive and more cumbersome. The mandate for persistent online connectivity can be a deterrent, especially for gamers in regions with patchy internet infrastructure or those who are frequently on the move.

Compatibility Concerns: While Denuvo is tailored to be harmonious with a broad spectrum of hardware setups and OS platforms, it's not devoid of compatibility issues. These can arise from:

Hardware or Software Conflicts: Specific combinations of components, drivers, or other software can, at times, be at odds with Denuvo or the associated game, leading to non-optimal game performance or crashes.

System Specifications: Games integrated with Denuvo might have certain system prerequisites for optimal gameplay. Falling short of these could result in potential compatibility hitches.

Piracy: Denuvo's prime objective is to combat piracy. However, pirated or cracked versions of games, which might have been tampered with or might be missing critical components, can encounter compatibility obstacles.

To further accentuate compatibility challenges, as newer CPU architectures are introduced annually by giants like Intel or AMD, Denuvo might lag in immediate adaptability, causing interim compatibility problems with some games. However, several games have employed a more lenient approach to DRM, including notable titles like 'The Witcher 3: Wild Hunt' and 'Minecraft'. Developed by CD Project Red, 'The Witcher 3' made a significant statement in the industry by opting not to use DRM [9]. The developers believed that treating their customers with trust would lead to higher sales and lower piracy rates. This philosophy starkly contrasts the prevalent belief in the industry. Despite

DOI: 10.54254/2755-2721/89/20241059

its lack of DRM protection, 'The Witcher 3' achieved commercial success, selling millions of copies worldwide. Similarly, 'Minecraft,' developed by Mojang, also employs a more relaxed DRM strategy. While the game requires an online verification during purchase, players can subsequently run the game in offline mode, demonstrating less restrictive DRM. Furthermore, Minecraft doesn't limit the installation and usage across multiple devices, which aligns with Mojang's philosophy of building an inclusive player community. Despite potential risks, the successes of 'The Witcher 3' and 'Minecraft' hint at the viability of a less stringent DRM strategy in certain contexts, sparking discussions about the balance between copyright protection and consumer freedom [10].

3. Conclusion

The evolution of DRM technologies, underpinned by advanced cryptographic techniques, has been integral in the growth and protection of the gaming industry. However, the development and implementation of these technologies are not without controversy and criticism. While DRM systems, such as Denuvo and online distribution platforms, have proven effective in thwarting piracy and safeguarding developers' rights, they have also faced backlash due to performance degradation, user inconvenience, and potential compatibility issues. There remains a pressing need to strike a balance between stringent DRM to protect developers' interests and a more lenient approach that respects consumer rights and ensures an optimal gaming experience. Interestingly, the success of 'The Witcher 3' and 'Minecraft' suggests that such a balance might be attainable, where consumer trust and freedom could serve as effective countermeasures to piracy. In the face of evolving technological landscapes and changing consumer demands, the gaming industry will continue to refine DRM technologies. This journey will necessitate careful navigation between the necessity to safeguard intellectual property and the obligation to respect consumer rights. As DRM technologies continue to evolve, it will be intriguing to observe the future trajectories they may follow, the challenges they may face, and the compromises they may need to make.

References

[1] Subramanya, S. R., & Yi, B. K. (2006). Digital rights management. IEEE potentials, 25(2), 31-34.

[2] Feigenbaum, J., Freedman, M. J., Sander, T., & Shostack, A. (2001, November). Privacy engineering for digital rights management systems. In ACM Workshop on Digital Rights Management (pp. 76-105). Berlin, Heidelberg: Springer Berlin Heidelberg

[3] Armstrong, T. K. (2006). Digital rights management and the process of fair use. Harv. JL & Tech., 20, 49.

[4] Colangelo, T. (2020). Digital Rights Management in video games: their impact on performance and the legal structure connected to them.

[5] Rump, N. (2004). Can digital rights management be standardized? IEEE Signal Processing Magazine, 21(2), 63-70

[6] Karthik, J., Amritha, P. P., & Sethumadhavan, M. (2020, July). Video Game DRM: Analysis and paradigm solution. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-4). IEEE.

[7] Burk, D. L., & Cohen, J. E. (2001). Fair use infrastructure for rights management systems. Harv. JL Tech, 15, 41.

[8] Ma, Z. (2017). Digital rights management: Model, technology and application. China Communications, 14(6), 156-167.

[9] Bechtold, S. (2003). The present and future of digital rights management–musings on emerging legal problems. Digital rights management: Technological, economic, legal and political aspects, 597-654.

[10] Zhang, Z., Pei, Q., Ma, J., & Yang, L. (2011). Game-theoretic analyses and simulations of adoptions of security policies for DRM in contents sharing scenario. Intelligent Automation & Soft Computing, 17(2), 191-203.