Thomas Waggoner | Logen Dickey | Ryli Botts

Professor Hang Zhang

I430 Security for Network Systems

4 December 2023

Reverse Engineering in Online Gaming

Abstract

Reverse engineering in gaming, particularly concerning multiplayer online games, presents a complex challenge to both cybersecurity and game integrity. While widely recognized for its role in emulating gaming consoles and exposing vulnerabilities in game codes, its most profound impact is observed in the online gaming sphere. This research delves into the intricate ways reverse engineering affects online multiplayer games, manifesting in unfair competitive advantages, security breaches, and intellectual property concerns. While our investigation predominantly centers on the online gaming community, we also acknowledge the broader implications across various gaming markets, albeit to a lesser extent. We scrutinize existing exploits and their consequences, assess the effectiveness of current solutions, and propose innovative approaches to mitigate these challenges. Our study aims to provide a comprehensive understanding of reverse engineering's role in online gaming and offer actionable insights for enhancing security and fairness in this dynamic digital arena.

Introduction

Have you ever found yourself immersed in an online multiplayer game, only to encounter a player whose abilities seemed beyond the norm? These exceptional abilities may stem from hacks and cheats, crafted by exploiting vulnerabilities revealed through reverse engineering. In

this paper, we delve into the myriad of challenges faced by both gaming companies and players when malicious actors leverage reverse engineering for their nefarious activities. Our research centers on solutions aimed at mitigating the impact of hackers who use reverse engineering to gain an unfair competitive edge.

In the initial sections of the paper, we acknowledge some legal and ethical concerns, then we lay the groundwork by highlighting the fundamentals of reverse engineering, particularly its application in exploiting gaming systems. We explore the diverse ways in which hackers employ reverse engineering with the intent of causing harm to companies and individuals within the gaming community. Furthermore, we delve into established methods that developers engage to reduce the likelihood of their games being reverse engineered.

In the latter part of the paper we delve into pre-existing solutions the gaming industry already employs as well as original ideas designed to combat reverse engineering and reduce hackers in the realm of multiplayer games. By combining observations on established practices and proposing original approaches, we aim to contribute to a comprehensive understanding of the challenges posed by reverse engineering in gaming and the ongoing quest for effective solutions.

Legal and Ethical Implications

When talking about the topic of reverse engineering games, it is important to keep in mind that the legal and ethical implications shape how players and developers interact with games. On the legal side, we want to protect developers and hope to guard their intellectual property and keep the integrity of gaming strong. While on the other hand, we also recognize that not all uses of reverse engineering are going to be used for malicious purposes (eg. emulating games to preserve their playability). In this battle of legal and ethical standing it is

hard to draw conclusion on what should be the standard, although there are practices currently in place that legally shield the integrity of some games.

One way to legally protect the integrity of video games is through Digital Rights Management (DRM), which is a way to ensure that users are not trying to pirate or access games/code that isn't protected under DRM. It does this by checking for an authentication when the user logs in, that the game reads and verifies is an authentic source. To ensure that DRM has legal implications former President Bill Clinton passed a law that went into effect in 1998 called the Digital Millennium Copyright Act (DMCA), that basically states anyone trying to violate a copyright will have legal consequences ("DMCA Notice: Everything You Need to Know"). This allows for intellectual property owners to now have a protection against piracy and many other forms of copyright infringement. That being said, this law has faced much pushback and is not supported by everyone in the community. Some believe that users should have the right to change code and alter other forms of games after they own it. As games get older, they can become no longer playable due to many reasons, this creates a user base that wants to play older games without access to the console. Game preservationists achieve this by using game and console emulation, created using reverse engineering.

Emulation of gaming consoles and games can be something that is useful to preserving video games. That being said, it can also be concerning to online gaming communities. While this practice is often used to preserve older titles that developers no longer support, due to the games no longer being financially viable, it inadvertently creates a complex scenario where online communities can access and modify these games that they do not legally own the rights to, often leading to unauthorized multiplayer versions that bypass standard online platforms. This is a risk as the developers of the original game now have no control over who is distributing and maintaining their content. This emulated version can have malicious code injected and compromise victim's machines.

As these emulated consoles evolve, the original creators lose control over their systems, due to the original hardware being incompatible with modern displays or the physical deterioration of the original units. While this enables a form of legacy preservation and community engagement, it simultaneously poses significant challenges to the integrity of online gaming ecosystems. Those skilled in reverse engineering not only can replicate games but also possess the capability to introduce hacks that can compromise the experience of all players involved. These emulated environments can lead to unfair advantages, compromised security, and potential revenue losses for developers. They disrupt the intended balance and competitive fairness in online gaming, raising critical concerns about maintaining a secure and equitable online space. To keep all games both new and old accessible and secure for generations to come, an open-source anti-cheat software that is broadly compatible with a wide variety of games is needed in order to insure the players and developers experience is not compromised in any way. This intersection of reverse engineering and online gaming communities highlights a crucial area of our study, focusing on the repercussions for both the players and the industry at large. The online emulation community is not supported by the law but many players see this as ethical to keep older games running after the developer support is done. These communities still want to remain protected by anti-cheat software that is open source so that they can implement it into older games to mitigate cheaters in their legally questionable endeavors.

Intro to Reverse Engineering

Reverse engineering involves deciphering machine code—the binary language of computers—to replicate the original functionality of the code. When you download a game you do not download the human readable code instead the computer downloads the machine code. Machine code is what allows computers to efficiently read the code that is not readable by people, this is because the human readable code used to develop the game has been

converted to hexadecimal bytes. Through meticulous analysis, individuals can decipher the intended functionality of the original, human-readable code through an intermediate coding language (assembly) that has a simple set of commands it can utilize. This allows the reverse engineer to understand where the game stores important information and then rebuild the game in the original coding language such as C++ or Java. Once someone gains access to the source code, they can put in anything they want into the game. This not only grants players an unfair advantage in multiplayer games but also poses the risk of inadvertently banning innocent players who unknowingly engage with these hackers. There have also been a few reported cases of hackers taking control of other players' computers through the use of exploits obtained through reverse engineering. In some extreme cases, as reported in the Dark Souls 2 incident, hackers have been able to gain complete control over other players' computers, leading to serious security breaches including the theft of passwords and sensitive data. (Troughton)

The hackers that utilize cheats attempt to recreate the machine code that the game is feeding to the computer. This is where reverse engineering comes into play. Due to the myriad forms of reverse engineering, completely preventing access to a game's source code remains an elusive goal. “Any code that executes successfully can be reverse engineered” (Sikorski and Honig 327). Nevertheless, despite the impossibility of absolute security, various methods exist to mitigate the risks and protect against such hackers. The gaming community and developers are constantly researching and implementing new fortifications to defend themselves from the adverse effects hackers impose. As observed in popular games like PUBG and Overwatch, cheating is not only rampant but also significantly detrimental to the gaming experience, with the potential to drive away a game's player base (Franceschi). Given the pervasive threat posed by these hackers, virtually all multiplayer games face a high risk of being targeted.

Common Hacks and Cheats

You might wonder, what specific exploits and cheats contribute to these challenges? To put it simply, there are hundreds of instances that can be unique to even the game itself resulting in too large of a list to put here. Yet, there exist several versatile and widely recognized cheats that are likely familiar to many. Firstly, wallhacks are one of the most commonly used cheats in games today (“BlackMirror: Preventing Wallhacks in 3D Online FPS Games”). These wallhacks profoundly affect the player base, experience, and community of online games. By allowing players to see through solid objects, wallhacks disrupt the intended balance and competitive fairness of the game. This not only undermines the skill and strategy that form the core of the gaming experience but also creates an environment of mistrust among players. When players suspect or know that others are using such cheats, it diminishes their engagement and satisfaction with the game. This erosion of trust leads to a decline in the game’s community, as fair players become disillusioned and may ultimately leave the game, seeking a more equitable gaming environment.

Aim-bots are another common hack. This allows players to have increased precision in shooting games as the in-game reticle will either be slightly guided toward an enemy hit box or rapid snap towards enemies through the wall when implemented with wall hacks. This can make some online matches nearly impossible to win as the hacker can achieve precision that a human cannot compete with, essentially making the game unwinnable for the other team. By tampering with the game's fundamental mechanics, aimbots can open pathways for more malicious exploits, including the theft of personal data. When hackers gain such deep access to manipulate a game's core functions, they may also acquire the capability to access sensitive player information. This not only disrupts the competitive balance but also poses a significant threat to the cybersecurity of individuals. The use of aimbots, alongside all other hacks/cheats

discussed here, becomes a dual concern: it undermines the integrity of the game and potentially jeopardizes the personal security of its players.

Popular games ranging from PUBG and World of Warcraft to Dark Souls have all grappled with numerous exploits. Each example of these hacks is just one hacker's interpretation as there are multiple different ways to implement any one genre of hack so as a developer patches their game to defeat one hack two more will take its place shortly. Although these examples represent only a fraction of the total games affected, they underscore the severity of the impact on both players and companies. The exploits that are found via reverse engineering can make hackers millions of dollars, simply by selling packaged cheats for online multiplayer games. This immensely hurts game developers as many people stop playing games after encountering even a small amount of cheaters, this causes developers to spend company resources to find the newest implementation of cheats, sometimes hurting regular players as they are hit with false-positives. Some individuals, such as well-known streamers, can serve as reliable influencers for games, attracting thousands of purchases. The lack of endorsement from prominent streamers can lead to a domino effect, resulting in the loss of millions in potential sales, driven by word of mouth and social media influence. Not only are potentially millions of purchases forfeited, but the overall trust and reputation for the game company could be destroyed, ruining any endeavors they may pursue later on (or affecting all their current ones). This is why keeping game integrity is a key issue in designing a well functioning game and can make the difference between having a successful game that earns millions of dollars a year or one that is quickly regarded as a pool of hackers and cheaters.

Several other types of cheats have become notoriously widespread, deeply disrupting the gaming community at large. Among these, aimbots and speed hacks stand out for their capacity to erode the core principles of fair play and competition. Aimbots, programmed to provide players with unnaturally precise targeting, strip away the skill-based aspect of games, leading to a hollow and unfulfilling experience for both the cheater and their opponents. Speed

hacks, altering the speed at which a player moves within the game, similarly distort the gameplay dynamics, creating an uneven playing field where legitimate players cannot compete on equal terms. These cheats not only fracture the community's trust in the game's integrity but also provoke frustration and disillusionment among the player base. The rampant use of such cheats in popular games like Fortnite and Apex Legends exemplifies their pervasive impact, turning potentially thrilling and competitive matches into lopsided affairs devoid of genuine challenge and enjoyment. This widespread disruption necessitates a concerted effort to maintain the delicate balance of competitive fairness, underscoring the urgent need for effective countermeasures against such pervasive and community-damaging cheats.

In order to create these kinds of cheats, specifically for wallhacks, hackers start by analyzing the game client software, which includes all the data and executable code necessary for the game to run on a player's computer. Through reverse engineering, they then examine the game's compiled code to understand how it processes, renders graphical elements, including player models and environmental structures (graphical elements being specifically for cheats like wallhacks). Subsequently, they analyze the game's memory during runtime to identify data structures representing players, the environment, and other in-game elements. After locating the memory, they then alter how the engine draws the world, modifying certain aspects and objects to be seen through walls (like players or their outline). The reverse-engineered wallhack is now complete and packaged into a script, mod, or third-party software that allows for anyone to be able to easily download and use. This method of reverse engineering serves as a base to most cheats and hacks that are created, and is not just limited to wallhacks.

The nefarious reach of hackers in online gaming extends beyond gameplay disruption, venturing into the life destructive realm of personal data theft. This is not a hypothetical threat but a stark reality, as demonstrated in severe incidents like the Dark Souls 2 security breach. Hackers, exploiting vulnerabilities exposed through reverse engineering, gained alarming levels of access to players' computers, pilfering sensitive data such as passwords and personal

information (Troughton). This incident lasted for over a year. Such incidents not only violate the privacy of individuals but also shake the confidence of the entire gaming community in the security of their online environments.

These breaches are a grim reminder of the intertwined relationship between gaming enjoyment and cybersecurity. They can affect things as sensitive as your bank accounts, resulting in physical monetary things like your own money being at risk. As we explore further, the challenges in ensuring cybersecurity become apparent, revealing a complex landscape where protecting against cheats is as much about safeguarding personal data as it is about maintaining game integrity. This intricate interplay necessitates a deep dive into the sophisticated and ever-evolving domain of cybersecurity measures, aiming to shield both the virtual and real-world identities of players from the malicious intents of hackers.

Industry Solutions

Therefore there is a need for a system that can adapt to multiple types of exploits, not just a specific signature for those being currently abused. The community surrounding hacking is far too large for any one game company to take on by themselves. A well established anti-cheat system that can address multiple facets of this epidemic are needed to keep the integrity of multiplayer games. While the security regarding online gaming is evolving daily, there are several well-established solutions designed to combat cheaters in gaming. As this is still an ongoing issue we will outline certain features that are desirable in each one of these systems as well as the shortcomings for each one of the implementations. Notably, we found an anomaly based Intrusion Detection System (IDS) proves highly effective by evaluating specific factors such as speed, acceleration, accuracy, and items that a normal player should not typically attain. For example, a player moving at an impossibly high speed or consistently achieving perfect accuracy will typically trigger the IDS. Instances of abnormally high performance in these

categories, especially when repeated, often indicate an individual injecting code obtained through reverse engineering of the game's source code. To illustrate, a player consistently achieving impossible levels of acceleration or possessing rare items beyond the game's legitimate parameters raises red flags. In response to repeat offenses, accounts can be banned, a desirable outcome as it relies on anomaly detection, effectively capturing day zero exploits—exploits discovered and deployed before the gaming community or developers become aware of them.

While the points listed are just a few of what an anomaly based IDS might look for, the power of AI can help gather more data on each individual player. A project from modl.ai is planning on gathering a variety of data from players so that it can characterize each player on a specific basis on parameters that wouldn't normally be thought of as cheat related like reaction time. This would be incredibly difficult for a person to find data points that are associated with cheaters and set up multiple IDS factors. Modl.ai has a foundational idea of knowing the individual player because "If we understand what part of the player base is cheat-prone and cheat-sensitive, we can generate one model that works very well because it ignores a large segment of players." (modl.ai) allows for personalized cheat detection that takes each player's skill and unique playstyle into consideration in order to determine legitimacy of each player.

Unfortunately, certain hacks, like wall hacks (which allow players to see through walls), remain largely unseen by IDS due to their less detectable nature. Wall hacks, being more discreet, manipulate the visual aspects of the game rather than altering performance metrics like speed or accuracy. Additionally, these systems become vulnerable if attackers are aware of the thresholds triggering the IDS, allowing them to stay just below the allowed limit. For instance, an attacker who knows the precise speed or accuracy values that trigger the system might deliberately keep their cheating behavior within the undetectable range, evading the IDS. These nuances highlight the ongoing challenge of staying one step ahead in the cat-and-mouse like game between game developers and cheaters.

With the games streaming market experiencing substantial growth and currently valued at over $9 billion globally (Mordor Intelligence), leading companies are increasingly adopting game streaming as a strategy to enhance security measures and expand their audience reach. This method effectively safeguards the game's source code from reverse engineering, thereby providing a solid line of defense against potential security breaches. The source code is securely housed in a server room under the company's control, allowing for stringent monitoring of each game for any indications of unusual activity. Rather than relying on the user's device for game computations, the responsibility is shifted to the company's server. After processing the user's input commands, the server then delivers the game's visuals, further contributing to the ongoing expansion and evolution of this thriving sector.

However, these increased security measures come with trade-offs. The strength of a user's internet connection directly influences the delay between your actions and on-screen responses, potentially disrupting gameplay during internet outages or periods of high network traffic. Additionally, developers are faced with the challenge of managing the computing power required for each game, leading to a significant uptick in production costs. Consequently, sustaining servers for older games becomes a formidable task, possibly rendering them unplayable if a company deems them no longer financially viable. This then leads to the aforementioned problem of emulation and game preservation. All of these issues combined make it hard for companies to employ, even for the largest businesses such as NVIDIA GeForce Now, Google Stadia, Playstation Now, and others as adoption has been growing but streaming services such as Stadia, from one of the industry leaders Google, have been canceled. Regardless of hardship this will likely become one option for fair gaming platforms as many companies are seeing the growing market and potential solution for cheating all in one.

Our solutions

Intel has implemented Software Guard Extensions (SGX) which allows for “hardware-based memory encryption that isolates specific application code and data in memory” (Intel) and AMD has a very similar process called Secure memory encryption to encrypt their memory as well. This means that even if you have root access to the machine you cannot access certain aspects of the software in the memory. Developers can also choose what operations are being stored in this encrypted section of memory called an enclave. This allows for certain assets that are unchanging like building locations and map layouts to remain unencrypted as well as keeping enemy player locations secret until certain conditions have been met like players having a clear line of sight to the enemy. This implementation allows game companies to still have the processing power be handled on the client side while keeping the server computation at a minimum. SGX is a somewhat old technology as well that has not been utilized to its full potential as it has been a part of Intel since the 6th generation originally released in 2016. This is great as Intel CPUs have the highest market share for any pc processor as well as having multiple supported years of CPUs that support SGX means that many games can implement enclaves in their game without disrupting their user experience. There are still some downsides as developers would have to update older games to implement these two systems as well as potentially having two separate versions for AMD and Intel depending on how each system handles their encryption process. Also this encryption and decryption process takes more time as the computer decides when the player is able to access this information. As CPUs are becoming faster this time delay can be negligible depending on the developers implementation. Memory encryption is a process that we believe is being underutilized in the current gaming landscape and could be a huge step in eliminating cheating on people’s personal computers.

Waldo.vision has a lot of the aspects that we are looking for in an anti-cheat system. This is an open source software that aims to not only analyze player stats but also player behavior. The team at waldo.vision are attempting to use AI learning to catch cheaters based on video clips of the hacker. This means that it can dynamically change to new cheats as they come out as new video evidence is uploaded to the platform. This also eliminates the worry for signatures for specific cheats as it analyzes player behavior through video evidence instead of analyzing altered game code. As this stands now it is currently being developed with a community of volunteers and donations.

Still there are downsides, This is dependent on player feedback and player submissions. This means that some of the data will be imperfect as well as having a delayed reaction time as it learns to determine new cheats that try to break the systems by acting more human-like. There is also the concern that this does not catch the cheater as it is happening; it is currently run on a reactionary basis where the clips are uploaded after the match is concluded. This unfortunately means that there is no way to currently have waldo.vision track the players as the match is unfolding. This is a promising new technology and will provide a great option for games in the future when completed.

Conclusion

Reverse engineering is a complicated process that takes lots of time and effort from a dedicated community regardless of whether they are intending to use the technology for game preservation or implementation of cheats. A system that can help mitigate cheating in online games is needed for both current and previous gen games to preserve the fairness of gaming. That’s why an open source software like the waldo.vision project for all generations of games is needed. Newer games still in development should be utilizing memory encryption to prevent

development of more hacks as it can keep a level playing field for all players in nearly every gaming experience.

Citation Page

The Workshop | *RE for Beginners*, https://www.begin.re/the-workshop. Accessed 9 November 2023.

“BlackMirror: Preventing Wallhacks in 3D Online FPS Games.” *Byoungyoung Lee*, https://lifeasageek.github.io/papers/seonghyun-blackmirror.pdf. Accessed 9 November 2023.

“DMCA Notice: Everything You Need to Know.” *UpCounsel*, https://www.upcounsel.com/dmca-notice. Accessed 3 December 2023.

Franceschi, Lorenzo. “Inside The 'World's Largest' Video Game Cheating Empire.” *VICE*, 1 June 2021, https://www.vice.com/en/article/93ywj3/inside-the-worlds-largest-video-game-cheating-empire. Accessed 30 November 2023.

Han, M. L., et al. “Cheating and Detection Method in Massively Multiplayer Online Role-Playing Game: Systematic Literature Review.” *IEEE Xplore*, IEEE Access, 2022, https://ieeexplore.ieee.org/abstract/document/9766355. Accessed 30 November 2023.

Intel. “Intel.com.” *Take Control of Protecting Your Data*, Intel, 2021, https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html. Accessed 1 December 2023.

modl.ai. “Cheat Detection Bots How to Detect Cheaters in Video Games Using Machine Learning.” *modl.ai*, 21 February 2022, https://modl.ai/detect-cheaters-using-ml/. Accessed 30 November 2023.

Mordor Intelligence. “Game Streaming Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028).” Mordor Intelligence, 2023, https://www.mordorintelligence.com/industry-reports/game-streaming-market. Accessed 1 December 2023.

Sikorski, Michael, and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012. Accessed 9 November 2023.

Troughton, James. “Dark Souls 2 Servers Are Back, But Still Unsafe.” *TheGamer*, 26 October 2022, https://www.thegamer.com/dark-souls-2-servers-are-back-but-still-unsafe/. Accessed 30 November 2023.