Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/53/20241371

Application of cyberspace security in video games industry

Yuqi Jin

School of Cyberspace Security and Information Security Law, Chongqing University of Posts and Telecommunications, Chongqing. China

2020212405@stu.cqupt.edu.cn

Abstract. While video games are becoming an increasingly popular worldwide industry, there is a growing number of cheaters who exploit the flaws and weaknesses of games to gain advantages or earn money. This initiates a conflict between the 'black hat' and 'white hat' players. This article provides a comprehensive classification of cheats and anti-cheats in video games, accompanied by vivid illustrative scenarios. In terms of cheat classification, there are two main categories: Generic cheats, and those of special relevance to online games. Each sub-category will be accompanied by examples or explanations of the current situations. In the section on anti-cheating measures, a table will be provided to illustrate general methods to counter common cheats. This section also includes some novel and creative anti-cheat methods that utilize different technologies to address the issues. This paper also discusses the investigation of applying artificial intelligence (AI) to combat malfeasance by some researchers. Finally, the conclusion provides a general summary of the current anti-cheat situation and presents some divergent ideas for addressing cheating.

Keywords: Cyberspace security, video games, anti-cheat, cheaters.

1. Introduction

As pandemic spreading around the world, more and more people prefer to stay at home. As a result, indoor entertainments become prevalent. Video games, which need to be run in computers, switches, smart phones or other electronic devices, perfectly fit in with the condition. And video games are extremely attractive, or even addictive due to their fascination. Moreover, many people start to play online games to build connection with others and make new friends, which satisfies their social demand while staying at home. Therefore, video games have become one of the most popular domestic recreations in the world.

However, because of fast development of video games, there are multiple problems coming up in this industry. For example, game cheating—players use unofficial avenues to get huge advantages to win the games, exists in almost every game. According to a report given by Irdeto Global Gaming Survey, globally, 8% players think their game experience is always negatively impacted by cheating; 18% players think their game experience is often negatively impacted by cheating and 33% players think their game experience is sometimes negatively impacted by cheating [1]. And these numbers went up in some Asian countries [1]. The action of hacking has a tremendous impact on industry. 48% of players would buy fewer in-game content because of knowing other gamers were cheating, which straightly

DOI: 10.54254/2755-2721/53/20241371

damage a company's income [1]. Moreover, it will also damage company's reputation, which is of vital importance to a company's future.

Since the commencing of multiplayer online video games, the war of cheating has never ended. Because some of the codes inevitably meet mistakes and currently there are not a general way to solve them. One way to solve the problem is to set code rules and apply them to every line, which is effective but cumbersome for programmers. Another way is to use professional software to check the program, which is plausible but expensive, since cyberspace security isn't common knowledge. The development of anti-cheat systems has consistently mirrored a cat-and-mouse dynamic, as new cheating methods are continually devised to evade detection by the game's anti-cheat technology [2]. Identifying newly created cheat programs stands as a central challenge in anti-cheat advancement. For instance, if cheat-detection code is embedded within the game client and cheaters manage to find a novel way to bypass detection, developers must then enhance the anti-cheat measures, initiating a cycle that persists as long as the game remains active online. In this regard, the process of anti-cheat development closely parallels the evolution of antivirus software [2-4].

Some of the cheaters use software which they acquire from the internet, which are free or charged. Others use hardware like U disk or specific computer hardware, which is harder to detect from anti-cheat system.

In order to detect and eliminate cheating, game companies need to utilize cyberspace security knowledge to defend their products from permeation of hackers. This article collects many different types of cheats and diverse anti-cheat solutions from lots of previous articles. The cheats and anti-cheats will be classified and briefly explained in the article.

2. Background introduction

2.1. Cheat classification

There are hundreds of or even thousands of cheats. Table1 is one of the classifications and some examples of online game cheating.

Table 1. Common cheating forms in online games [5]

Type	Label	Cheating Form
Of special relevance to online games	1	Cheating by Exploiting Misplaced Trust
	2	Cheating by Collusion
	3	Cheating by abusing the Game Procedure
	4	Cheating related to Virtual Assets
	5	Cheating by exploiting Machine Intelligence
	6	Cheating by Modifying Client Infrastructure
	7	Timing cheating
Generic	8	Cheating by denying Service to Peer Players
	9	Cheating by compromising passwords
	10	Cheating by exploiting Lack of Secrecy
	11	Cheating by exploiting Lack of Authentication
	12	Cheating by Exploiting a Bug or Loophole
	13	Cheating by Compromising Game Servers
	14	Cheating Related to Internal Misuse
	15	Cheating by Social Engineering

On the client view, many tricks require falsifying with game code or configuration data [5].

DOI: 10.54254/2755-2721/53/20241371

2.2. Of special relevance to online games

Cheating by Exploiting Misplaced Trust

This type of cheat basically relies on the over-trust from the server on client. This mistake happens mostly in Offline due to most of these cheatings don't damage others' interest. And it only changes elements in the game. However, in online games, this mistake could be destructive because the server is actually protecting the cheater by mostly trust.

Cheating by Collusion

This type of cheat is an anthropic one. Mostly it is not related to technical cheat, but related to collusion cheat. For example, in battle royale games, where players group to gather weapons and tools to fight against other groups to win the game, there exist this type of cheatings, which some of groups cooperate together and not fight against each other to get number advantages. And this even happened in professional games. For example, in one of the professional competitions of game Apex in 2023. There are multiple international participants. And some of the groups that come from the same country collaborate with each other. Not in a blatant way but being quiescent to it that not shooting each other. And there was no penalty come up, since it was hard to judge whether they colluded or not.

Cheating by abusing the Game Procedure

This type of cheat sometimes happens by accident, and sometimes by intention. Cheaters use the flaw in the game rules or mechanisms to get advantages. Consider, for instance, the popular game Valorant, where a player might be temporarily away from their keyboard (AFK) during the initial round. If their teammates secure a victory in the opening round, the player will promptly return. However, in the event of their teammates facing defeat in the first round, the player may choose to disconnect. Consequently, their teammates may opt to initiate a vote for a game remake, as they are disinclined to engage in a 4v5 scenario. The reason why these cheaters do this is to predict the possibility of winning and decrease losing games in order to get better teammates and rank.

Cheating related to Virtual Assets

This type of cheat always happens out of games. And it causes serious damage to the economy of companies and individuals. Cheaters will use varied ways to get other's in-game products. For example, in VR-CHAT, a game where people have conversations in assorted virtual scenes with their virtual characters, there are many character skins were made by others and charged for fee. Cheaters could copy these skins if their orthodox owners forget to lock the copy-right. And once cheaters get these skins, they could sell them in a lower price to others and lead to huge problems.

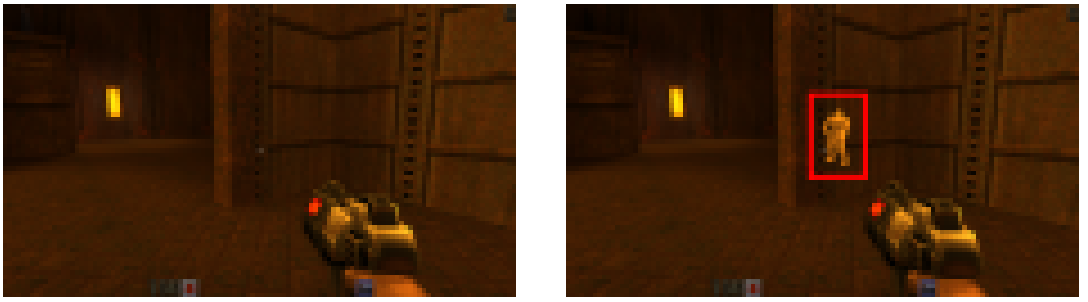
Cheating by exploiting Machine Intelligence

This type of cheat uses artificial-intelligence (AI) to analyze data in games. And it's hard to detect because it doesn't cross most edges. It just uses the information which cheaters get. For example, by using this cheat in FPS games, cheaters can flick their crosshair into enemies' heads to get more effective kills. And in card games, AI could predict the win rates of each play and tells cheaters.

Cheating by Modifying Client Infrastructure

A player can engage in dishonest behavior without impacting the game programs, configurations, or client-side information by manipulating the client infrastructure, which may include device drivers within their operating system [5]. This type of cheat sometimes doesn't break the game rules but changes some of the in-game elements. For example, there are many games that sell gun skins or character skins to players. Cheaters might change their client infrastructure to make their stuffs change skins into whatever they want. And others see cheaters' stuff skins like a default one. This type of cheat could also change walls in game to make them transparent. Wall hack tells cheaters where every opponent is and show them directly on their screen. Mostly, opponents will be shown in pure color outline. Figure 1 is one of the examples of such cheat.

DOI: 10.54254/2755-2721/53/20241371



(a) Benign view (b) wallhack view

Figure 1. An instance of wallhacks [6]

Timing cheating

In certain real-time online gaming scenarios, an unscrupulous participant may delay their own action until they possess full knowledge of all their adversaries' movements, thereby gaining a substantial advantage. This strategy, known as the 'look-ahead trick,' falls under the category of timing manipulation cheats. [5]. This type of cheat can also backdate other players' movement. For example, in FPS games, when some normal players peek after walls and fall back, cheaters could shoot their previous body which shown in cheaters' screen, and this shot deals damage to the players or could even make kills.

2.3. Generic

Cheating by denying Service to Peer Players

This type of cheat is one of common cheats in online games. By making other player lagging in the game, cheaters could gain huge advantages. And the ways of attack could be DDoS attack or other attacks that destroy website connection. DDoS attack means some cheaters use Distributed Denial of Service (DDoS) attack to make normal players forcedly disconnected from server and the players cannot reconnect back (Figure 2).

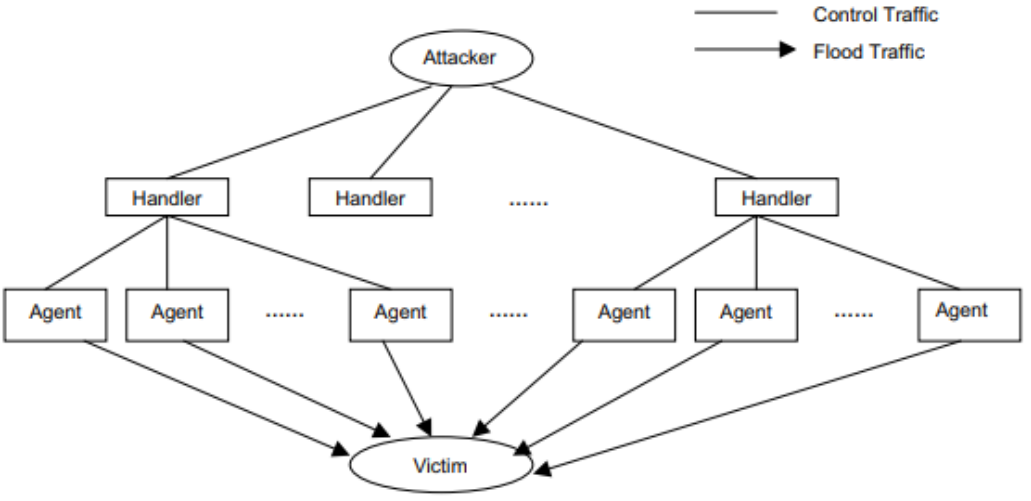


Figure 2. DDoS attack [7]

Cheating by compromising passwords

A passphrase often serves as the gateway to a player's complete data and access privileges within an online gaming system [5]. A cheater can get access to the victim's data and authorization in the gaming system by compromising a password [5]. This type of cheat happens mostly in Internet Café, where many customers login their own accounts in public devices. Cheater could implant virus in these devices, and once others login their own accounts, they will be delivered to the far away hosts.

DOI: 10.54254/2755-2721/53/20241371

Cheating by exploiting Lack of Secrecy

Tampering can occur by intercepting plain text communication packets and manipulating the conveyed game events or orders transmitted across the network [5]. By doing so, cheaters can not only observe but also alter, remove, or inject fraudulent game events or commands into the network stream. This illicit activity undermines the integrity and fairness of the gaming experience, highlighting the importance of robust security measures in online gaming systems.

Cheating by exploiting Lack of Authentication

This type of cheat could be exerted by lack of verification. And it is because of the bugs of some Internet protocol that set rules of sending messages or information to other. Cheaters could use software to pretend like a real server or client, and thus skip some verification to change the information of other players without permitted.

Cheating by Exploiting a Bug or Loophole

This type of cheat is one of the most usual cheats in industry. Since game designers focus more on game rules and experiences, they could be lack of experience on anti-cheat, which make their games quite vulnerable to cheaters and could be easily take control by cheaters. For example, some cheaters use scripting which could implement into some weak defensive games, and it permits cheaters to respond to opponent moves correctly and promptly [8].

Cheating by Compromising Game Servers

Once a cheater has gained access to the game host systems, he can tamper with game server programs or modify their specifications [5]. This sometimes happens in many online games like GTA5 or Apex, on which cheaters paralyze game servers in professional competition or official game while streaming.

Cheating Related to Internal Misuse

A game operator often has system administrator access. It is simple for an insider - a game operator personnel - to misuse this privilege [5]. For instance, he might manipulate the game database on the server side to generate exceptionally powerful characters, often referred to as "super characters."

Cheating by Social Engineering

Deceivers often employ tactics to mislead a player into believing that an enticing or troublesome event has occurred, leading them to believe that they need to provide their ID and password. Blizzard has released advice for avoiding similar frauds on its famous Battle.net website, demonstrating that this type of cheating is a genuine issue [5]. This type of cheat often happened in some popular games, where number of players believe their luck. And this type of cheat could even evolve into a more secretive form. For example, in FPS game CS:GO, it was launch on game platform steam, where there is a huge e-market where players exchange their in-game props like gun-skins, rare cards, character skins, potions and so on. Cheaters could inveigle innocent players to click their unknown link and login in on fake platform, which seemingly look like a normal login UI. And after players login the platform, cheaters could get over control of players accounts.

3. Anti-cheat method

There are colossal ways of anti-cheats, in Table 2, it gives a general classification of divergent solutions to cheat.

Table 2. Game cheats and their possible solutions [9]

Cheat	C/S	PB/V AC2	AS	NEO/SEA	RACS
Game Level					
Bug	•		•	•	•
Application Level					
IE, IC	•				•
Bots/reflex enhancers		•			
Protocol Level					

DOI: 10.54254/2755-2721/53/20241371

Table 2. (continued)

Suppressed update, Timestamp Fixed delay, Inconsistency Collusion	•		•	•	•
Replay, Spoofing	•			•	•
Undo	NA		•		NA
BO	NA		NA	NA	•
Infrastructure Level					
IE	•	•			•
PRE					

This article specifically reviews the anti-cheat of Client/Server (C/S) on Bug.

Anti-cheats on Bug

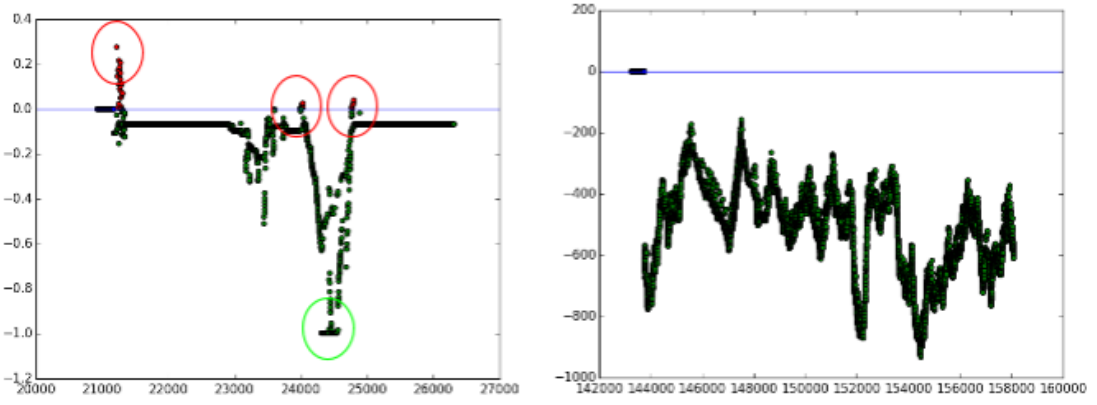
The first bug happened once an insect flew into a programmer's computer and caused malfunction. And it is continuously happening since ever begin. Nowadays, researchers use artificial intelligence to anti-cheats. Here are some examples:

(1) Host Based Anti-Cheats

Host-based anti-cheaters identify cheats by analyzing the host's system. These anti-cheats are often intrusive, digging into a host's RAM, hard disk, and hardware [4]. This type of anti-cheat is pretty popular in industry due to its depth in hardware and its effectiveness. For example, the VAC of company valve and the Vanguard of Valorant. Both of software need to be keep activated once the game is being played.

(2) Statistical-Based Anti-Cheats

This type of anti-cheats use data to simulate a players in-game performance. Both supervised training or unsupervised training is used in this area. In Figure3(a), a cheater's performance which is transformed into data, shows that cheaters always have abnormal performance. In other words, for example, in FPS games, some cheaters might flick their crosshair directly on the opponents' head while their previous performance shows that they are not good at other aspects of games. For example, their movement, crosshair placement, or consciousness in game could be low level.



(a) Cheater test data (b) Fair player test data

Figure 3. Example of statistical-Based Anti-Cheats [4]

Blackmirror, an alternative method to counteracting wall-hacks through trusted execution is introduced (Figure 4) [6]. Specifically, an anti-cheat system is proposed, eliminating the need for players to install dubious proprietary kernel modules on their devices, and relieving the game company from resorting to insecure obfuscation techniques to safeguard sensitive information [6].

DOI: 10.54254/2755-2721/53/20241371

(3) Novel detect

The design principles of AimDetect, along with the understanding of these recognized characteristics, are based on the observation that cheaters typically lack skill and are conspicuous [10]. It is quite frequently happened in FPS games, which cheaters behave abnormal or inhuman to cause other suspect their illegal actions. Therefore, while they may exhibit shooting proficiency comparable to skilled players, their performance in areas such as defense and situational awareness is more akin to that of average players [10]. Given the dynamic nature of FPS games, it proves difficult for aim bots to match the overall skill level of accomplished players [10]. However, there are also some exceptions in the industry. Some of the players or streamers even cheat for several years and just founded or yet to be found. For example, Streamer Ling Piao Miao was a great streamer in Chinese CS:GO and played a lot of competitions and won lots of prize. But in 2023, he was founded ban on server due to cheating. As a result, detection need to keep develop and renew to chase the cheat update.

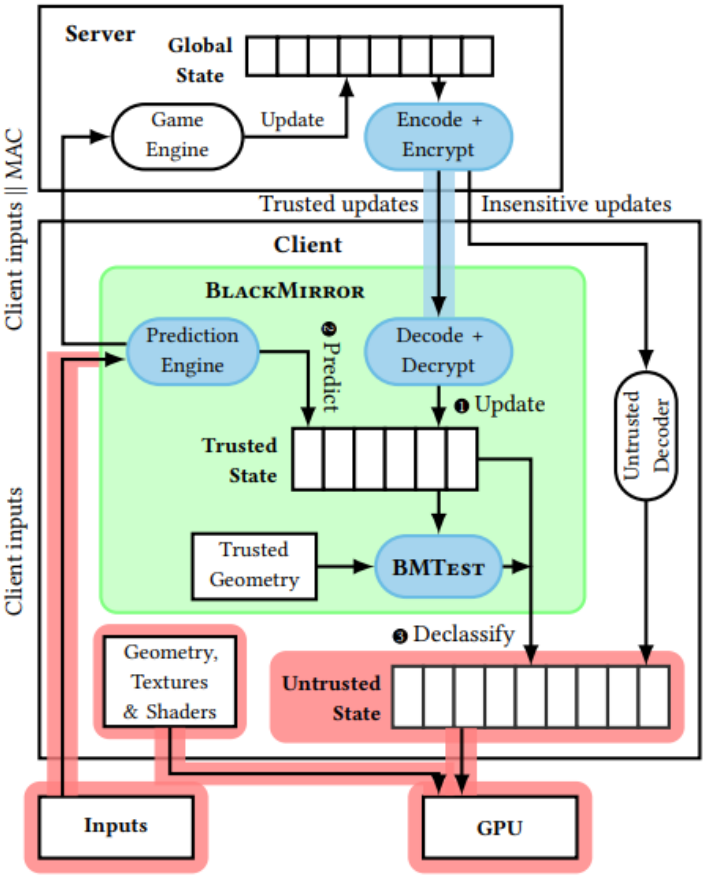


Figure 4. Overall construction of blackmirror [6]

4. Conclusion

All in all, the competition between the white hat and black hat is still going on. And there is no general solution to all hacking. Generally, there are two types of cheats, one is the anthropic cheats like colluding or conversation cheatings, another is the technical cheats like abusing of bugs, game flaws, or compromising. Cheating by Exploiting Misplaced Trust happens mostly because of the lack of wariness of server. Collusion cheating and exploiting game procedures occur when individuals disregard proper conduct and prioritize winning, regardless of whether it is achieved through fair means. Cheating related to Virtual Assets, cheating by compromising passwords and cheating by Social Engineering happen because of the lack of wariness of clients or players. Cheating by exploiting Machine Intelligence, cheating by Modifying Client Infrastructure, timing cheating, cheating by denying Service to Peer

DOI: 10.54254/2755-2721/53/20241371

Players, cheating by exploiting Lack of Secrecy, cheating by exploiting Lack of Authentication, cheating by Exploiting a Bug or Loophole and cheating by Compromising Game Servers are all technical cheatings that require code and website knowledge. Cheating Related to Internal Misuse is a special cheat that game designer cheat on his/her own games. The anti-cheats could vary from detection of cheats to analyzing performances. Host Based anti-cheats is a more predominant anti-cheat because it implants anti-cheat deeply. Statistical-Based Anti-Cheat is a relatively new anti-cheat that implement AI to analyze cheating. Blackmirror and Novel detect are more specific anti-cheats that deal with given cheats, for example, wall hack.

However, according to the survey [1], the ratio of cheating in Asian is higher than in Europe or US. The reason could be the difference on pressure of living. Because cheaters need to alleviate or get advantages for themselves in the virtual world. The main idea of anti-cheats might be a technical issue, but a more effective idea is to find why people cheats and willing to get advantages that not belonging to them and destroy others' game experience. And that might be a root problem, the intension of cheating.

References

[1] https://resources.irdeto.com/irdeto-global-gaming-survey/irdeto-global-gaming-survey-report-2 irdeto, "IRDETO GLOBAL GAMING SURVEY: The last checkpoint for cheating". 2018.
[2] Lehtonen, Samuli Johannes. "Comparative study of anti-cheat methods in video games." (2020).
[3] Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004): 39-53.
[4] Khalifa, Salman. "Machine learning and anti-cheating in fps games." Master's thesis (2016).
[5] Yan, Jeff, and Brian Randell. "A systematic classification of cheating in online games." Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games. 2005.
[6] Park, Seonghyun, Adil Ahmad, and Byoungyoung Lee. "Blackmirror: Preventing wallhacks in 3d online fps games." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020.
[7] Mirkovic, Jelena, Gregory Prier, and Peter Reiher. "Attacking DDoS at the source." 10th IEEE International Conference on Network Protocols, 2002. Proceedings.. IEEE, 2002.
[8] https://blog.irdeto.com/video-gaming/cheating-in-games-everything-you-always-wanted-to-know-about-it/, Reinhard Blaukovitsch, "Anti-cheat in video games: The A to Z", 2022
[9] Webb, Steven, Sieteng Soh, and William Lau. "RACS: A referee anti-cheat scheme for P2P gaming." Proceedings of the 17th international workshop on Network and operating systems support for digital audio and video. Association for Computing Machinery (ACM), 2007.
[10] Liu, Daiping, et al. "Detecting passive cheats in online games via performance-skillfulness inconsistency." 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2017.