

A Survey of Cheating Techniques in Online Games

Steve Webb

Mini-Project 3 – “Cheating in Online Games”
Advisor: Kang Li
CS7001

1 Introduction

In 1952, A.S. Douglas, a graduate student at the University of Cambridge, created the very first computer game – a modified version of Tic-Tac-Toe [5]. Douglas' creation was rudimentary by today's standards, but it generated a significant amount of interest. Consequently, over the course of the last half century, a great deal of research has been done to improve the entertainment value of computer games. Every year, new games are released that showcase the cutting edge in research areas as diverse as artificial intelligence, graphics, and human-computer interaction. However, despite all of these research efforts, the gaming community has largely ignored the threat posed by cheaters.

Traditionally, most computer games can be characterized as single-player games in which a human player competes against a computer player that utilizes artificial intelligence. In these games, cheating players only place the computer player at a disadvantage. However, with the emergence of network computing, a new paradigm of computer games has begun to gain in popularity: online multi-player games. In online multi-player games, a number of human players compete against each other by communicating over computer networks. Thus, in these games, cheating players harm human players instead of computer players. As a result, the gaming experience is ruined for non-cheating players.

As the world becomes more and more connected by high speed computer networks, the popularity of online games will continue to grow. In fact, it is estimated that by 2004, online gaming will become a 4.9 billion dollar industry [8]. Thus, as gaming companies begin to place more and more emphasis on online games, they must also focus on preventing cheaters from ruining the online experiences of their other customers. Otherwise, non-cheating players will refuse to play, and gaming companies will lose a significant amount of revenue.

This paper presents a survey of current techniques for cheating in online games. The remainder of this paper is organized in the following manner. Section 2 defines the behavior that

constitutes cheating and explains why cheaters cheat. Section 3 explains various cheating techniques and how they can be used to give cheaters an unfair advantage. Section 4 summarizes the conclusions.

2 Cheating Explanation

Defining the boundaries between what does and does not constitute cheating is a very difficult task. Many games offer a wide array of configurable options and customizations. Thus, some of these settings could be construed as cheating. For example, in some games, a player can change the color of their character's clothing in order to blend into the surroundings. This alteration gives the player the advantage of being harder to detect, but every player has the option of using this setting.

Using the previous example as a guideline, cheating can be defined as any action taken by a player to obtain an unfair advantage over other players. By this definition, the previous example would not be characterized as cheating because the clothing color option is part of the original game. However, if a player was only able to change this option with a mechanism outside of the game, it would be considered cheating because that player would have an unfair advantage over other players.

Understanding what constitutes cheating is important, but it is equally important to understand what motivates cheaters to cheat. Cheaters' motivations can be grouped into three categories: the desire to ruin others' online experiences, the thrill of victory, and money. First, many cheaters cheat strictly to ruin the online gaming experience for others. As Pritchard states in [4], "Cheaters get their kicks out of ruining the experiences for other people." Second, a large number of cheaters cheat because they want to win without practicing as much as legitimately good players. They play games for the same thrill of victory as everyone else; however, they win by cheating rather than by skill. Finally, some cheaters cheat because money is involved. For

example, the recent popularity of games such as Ultima Online [22] and EverQuest [11] has resulted in the auctioning of virtual characters and assets on eBay [9].

3 Cheating Techniques

Cheating techniques are typically implemented in one of three ways: client hooks, OpenGL wrappers, and hard-coded files [16]. Client hooks insert lines of code directly into the game as it is running in memory. OpenGL wrappers modify the functionality of OpenGL drivers so that graphics are drawn differently. Hard-coded files are typically dynamic linkable libraries (DLL) or configuration files that have been modified to alter the game's behavior.

Before an effective solution can be discovered for online game cheating, each of the problems must be enumerated. Thus, the following categories can be used to describe the various ways in which individuals cheat in online games.

3.1 Bug Exploitation

Games are fun and exciting, but they are not immune to the bugs and flaws that plague other pieces of software. Unfortunately, in some cases, these bugs can be leveraged by cheaters to gain an unfair advantage over other players. The following examples illustrate specific bugs that have been exploited by cheaters.

3.1.1 Bad Randomness

Many games rely on random events to ensure fairness. For example, card games such as Bridge and Poker require their deck of cards to be shuffled thoroughly before each new hand so that none of the players have an unfair advantage. Traditionally, computer games accomplish this shuffling with a pseudorandom number generator [13]. If the game's number generator is flawed

or the implementation of the shuffling algorithm is incorrect, the cards will not be dealt in a random fashion, and fair play will not be preserved [25].

3.1.2 Escaping

Most online games associate a rating with each participating player, which serves as an indicator of that player's skill level. This rating is typically calculated based on the player's record of wins, losses, and unfinished games. However, some systems do not account for unfinished games when calculating a player's rating. As a result, cheaters are able to disconnect from games in which they are losing without it negatively affecting their rating. This technique is often referred to as escaping, and it allows cheaters to artificially inflate their rating [26, 25, 15].

3.1.3 Command Collision

In an online game, if network communications experience enough lag, the game must postpone the next turn until communications can continue normally. However, while the game is suspended, players are still able to interact with the game's user interface. Consequently, a player may execute a number of commands while the next turn is being postponed. Whenever the game finally resumes, it processes all of the player's commands (even duplicates) as if they were executed in a single turn. The most common exploit of this behavior is called the "construction-cancelled" bug. In this bug, a player cancels the construction of a building (or some other transaction involving game resources) repeatedly when the game is suspended. Then, once the game resumes, multiple cancels are processed, and the game returns the original resources to the player along with additional resources that the player did not previously possess [17].

3.2 Ability Augmentation

A number of games require quick and precise reactions in order to be successful. For example, First Person Shooters (FPS) such as Counter-Strike [6] and Quake III Arena [18] are dominated by players who possess quick reflexes and great eye-hand coordination. Typically, these talented players spend countless hours fine-tuning their skills, but cheaters want results with as little effort as possible. Thus, cheaters often turn to various unfair techniques to augment their abilities in games so that they can compete on the same level as legitimately good players. The following examples showcase some of these methods.

3.2.1 Aim Hack

In a FPS, a player's objective is to aim and shoot other players. The most important aspect of this process is the aiming because a shot to another player's head is much more lethal than a shot to the arm or leg. Thus, players with the best aim are consistently the most successful in these types of games. Cheaters desire accurate aiming abilities, but they don't want to spend time practicing. As a result, they use an aim hack (also known as auto-aim or aimbot) to attain aiming skills. Two main types of aim hacks currently exist, but both essentially provide the cheater with perfect aim. The first aim hack acts as a proxy between the cheater's game and the gaming server. When the cheater attempts to fire at another player, the aiming proxy inserts additional game commands to ensure the cheater is aiming directly at the nearest opposing player [17]. The second aim hack is actually added to the game, but it provides the same type of functionality as the aiming proxy. However, the second aim hack can be configured to move the cheater's crosshairs and fire automatically [16].

3.2.2 Speed Hack

Aim is very important in a FPS, but evading the aim of others is equally important. A player's aim is irrelevant if the player is killed before being able to shoot. Thus, to avoid being targeted, good players jump all over the screen, dodging bullets and frustrating other players. However, these maneuvers require a great deal of skill and practice – two things cheaters wish to bypass. In order to successfully avoid being targeted in these games, cheaters often employ a speed hack which increases the rate at which they can move in the game [16]. The logic behind this cheat is simple: the faster the target moves, the harder it is to shoot.

3.2.3 Anti-grenade Hack

Many games contain items that can be used to temporarily impair the abilities of other players. For example, in Counter-Strike [6], players have the option of using flashbangs and smoke grenades to momentarily cloud the vision of opponents. To combat this situation, cheaters utilize an anti-grenade hack to remove the visual impairment from the screen. Consequently, this cheat makes the cheaters immune to flashbangs, smoke grenades, and various other items that serve to impair the abilities of legitimate players [16].

3.3 Denial of Service

Most cheats are used to give cheaters unfair abilities during game play. However, the purpose of denial of service (DoS) cheats is to deny game access to legitimate players. Cheaters use these cheats for a couple reasons. First, if a cheater implements a DoS cheat against an opponent while a game is running, the cheater can force the opponent to be disconnected, receiving an easy victory in the process. Second, a DoS cheat can be used to prevent an enemy or a superior player from accessing the game, allowing the cheater to avoid playing specific players. The following examples illustrate various DoS cheats.

3.3.1 Lag Hack

In online games, network latency is fundamentally important because it determines how fast a player's commands are received by the game's server. Thus, the more network latency present in an online game, the less responsive the game appears to its players. As a result, game developers attempt to minimize the amount of information being exchanged between players and the game server to avoid network latency issues. However, cheaters can introduce an artificial amount of network latency by flooding another player's network connection with meaningless traffic [26]. This additional traffic serves two purposes for the cheater. First, it decreases the perceived responsiveness of the game for the non-cheating player. Consequently, the non-cheating player might feel compelled to leave the game due to the excessive latency and slow response time. Second, the additional traffic could potentially slow the non-cheating player's network connection to a point where the game perceives the player as being unresponsive. This would result in the player being disconnected from the game. Both of these scenarios result in an easy and undeserved victory for the cheater.

3.3.2 Invalid Login Attack

To access most online games, players must log into the game's server with their unique username and password. This login process authenticates players to the server, preventing cheaters from accessing accounts that don't belong to them. As an additional security precaution, some online games only allow a certain number of login attempts before the account is temporarily frozen. This precaution is typically implemented to help prevent online password cracking attacks such as the dictionary attack. However, this security feature allows a cheater to freeze non-cheating players out of their accounts. By purposely logging into an account with an invalid password, the cheater is able to freeze that account. Thus, a cheater can easily deny non-cheating players access to their accounts.

3.4 Knowledge of Classified Information

In many online games, a player's computer has knowledge of everything that is happening in the current game. For example, in real time strategies (RTS) such as StarCraft [21] and WarCraft III [24], a player's computer knows information about the other players in the game even if they cannot be seen by the player. The player is supposed to be unaware of this information until the player actually finds the other players. The player's computer has this information because it allows for techniques such as dead reckoning [1], and it is far more efficient than having the server constantly update the information known by the player's computer. However, despite the classified nature of this information, cheaters are able to leverage it to their advantage.

3.4.1 Map Hack

In a RTS, a player controls some number of characters which are used to accomplish various objectives – typically the destruction of the other players' characters. These games offer players a world in which their characters interact, but usually, each player's view of the world is restricted to the areas in which that player has explored. If a section of the world has not been explored by the player, it is covered by the “fog of war.” In this situation, the fog serves to conceal the classified information – the areas of the map not previously explored by the player. To exploit this scenario, cheaters employ a map hack which removes the “fog of war” regardless of whether or not the cheater has explored the entire map [17]. In doing so, the cheaters are able to obtain an unfair advantage because they have knowledge of classified knowledge.

3.4.2 Wall Hack

In a FPS, players are surrounded by various obstacles (i.e. walls, boxes, etc.), and they must maneuver around the map to find and shoot other players. In normal game play, players are

only able to see other players that are in their field of vision. This means that if players are hiding behind obstacles, they should not be visible to other players. Games show a player's field of vision by drawing each scene from back to front [17]. Therefore, if other players are hiding behind obstacles, the obstacles are drawn on top of them so that it appears as though they are not there. A cheater is able to exploit this situation by using a wall hack which draws the obstacles transparently. Thus, players that are hiding behind obstacles are no longer hidden because the obstacles appear to be transparent.

4 Conclusion

As online multi-player games continue to grow in popularity, the ability to prevent cheating will become increasingly important. This paper gave a clear definition of what cheating is, and it provided a number of motivations for why cheaters cheat. Additionally, the paper enumerated many of the cheating techniques currently being implemented by cheaters, categorizing them into four main groups: bug exploitation, ability augmentation, denial of service, and knowledge of classified information. By presenting these categories and specific cheating techniques, this paper should facilitate the continued research of more effective solutions to online game cheating.

References

- [1] J. Aronson, "Dead Reckoning: Latency Hiding for Networked Games," *Gamasutra*, 19 Sept. 1997, http://www.gamasutra.com/features/19970919/aronson_01.htm (current 8 Nov 2003).
- [2] M. Bacarella, "Anti-Cheat Mechanisms: Limited Trust in Online Gaming Communities," <http://michael.bacarella.com/papers/netoftrust.html> (current 8 Nov. 2003).
- [3] N. Baughman and B. Levine, "Cheat-Proof Payout for Centralized and Distributed Online Games," In *Proceedings of the 20th IEEE INFOCOM Conference*, 2001.
- [4] D. Becker, "Online gaming's cheating heart," CNET News.com, 7 June 2002, <http://news.com.com/2100-1040-933822.html> (current 8 Nov 2003).
- [5] M. Bellis, "The History of Computer and Video Games," http://inventors.about.com/library/inventors/blcomputer_videogames.htm (current 8 Nov 2003).
- [6] Counter-Strike website, <http://www.counter-strike.net> (current 8 Nov 2003).
- [7] E. Cronin et al., "Cheat-Proofing Dead Reckoned Multiplayer Games, In *Proceedings of the 2nd International Conference on Application and Development of Computer Games (ADCOG 2003)*.
- [8] S. Davis, "Why Cheating Matters: Cheating, Game Security, and the Future of Global On-line Gaming Business," In *Proceedings of the 2001 Game Developers Conference*.
- [9] eBay website, <http://www.ebay.com> (current 8 Nov. 2003).
- [10] Even Balance, Inc., PunkBuster website, <http://www.evenbalance.com/> (current 8 Nov. 2003).
- [11] EverQuest website, <http://everquest.station.sony.com> (current 8 Nov. 2003).
- [12] A. Kirmse and C. Kirmse, "Security in Online Games," *Game Developer*, July 1997.
- [13] D. Knuth, *The Art of Programming, Volume 2: Seminumerical Algorithms*, Third Edition, Addison-Wesley, 1998.
- [14] H. Lee et al., "Synchronization and Cheat-Proofing Protocol for Real-Time Multiplayer Games," In *Proceedings of the 2002 International Workshop on Entertainment Computing*.
- [15] K. Mørch, "Cheating in Online Games – Threats and Solutions: Version 1.0," Norwegian Computing Center/Applied Research and Development, 8 Jan. 2003, <http://www.nr.no/dart/projects/gisa/download/Cheating%20in%20Online%20Games.pdf> (current 8 Nov. 2003).
- [16] A. Moses, "Cheating – Multiplayer Gaming's Achilles' Heel?" <http://www.tomshardware.com/game/20030517/index.html> (current 8 Nov. 2003).

- [17] M. Pritchard, "How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It," *Information Security Bulletin*, Feb. 2001.
- [18] Quake 3 Arena website, <http://www.idsoftware.com/games/quake/quake3-arena> (current 8 Nov 2003).
- [19] N. Shachtman, "'Blizzard' of Cheaters Banned," *Wired News*, 12 Sept. 2002, <http://www.wired.com/news/games/0,2101,55092,00.html> (current 8 Nov. 2003).
- [20] A. Smith, "ASUS releases games cheat drivers (Boo! Hiss!)," *The Register*, 5 Oct. 2001, <http://www.theregister.co.uk/content/50/18870.html> (current 8 Nov. 2003).
- [21] StarCraft website, <http://www.blizzard.com/starcraft/> (current 8 Nov. 2003).
- [22] Ultima Online website, <http://www.uo.com> (current 8 Nov. 2003).
- [23] United Admins, "Why Cheating-Death is Different," <http://www.unitedadmins.com/cdeath-why.php> (current 8 Nov. 2003).
- [24] WarCraft III website, <http://www.blizzard.com/war3/> (current 8 Nov. 2003).
- [25] J. Yan, "Security Design in Online Games," In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003)*.
- [26] J. Yan and H. Choi, "Security Issues in Online Games," *The Electronic Library*, Vol. 20, No. 2, 2002.

This document was created with Win2PDF available at <http://www.daneprairie.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.