Cheating in Modern Computer Games: Methodologies and Prevention

Project Plan

Ronald Chan (3035374503)
20th September 2020

Supervisor: Dr. Chim T.W.
Contents

1. Background
   1.1 The Modern Gaming Industry
   1.2 The Video Game Cheating Industry
2. Objectives
3. Methodology
   3.1 Classification of different existing types of cheats
   3.2 Overview of common anti-cheat measures
   3.3 The future of game cheating and anti-cheating
4. Schedule and Milestones
5. References
1. Background

1.1 The Gaming Industry

In the past decade, due to the increase in the popularity and ease-of-access of the internet, the computer video games industry has transformed from mainly accommodating for single-player games, into focusing mainly on the production of multiplayer online games. In fact, according to Steam’s statistics on top games by current player count in September, 2020 [1], the top 5 games are all multiplayer online games, which shows how the video game industry has evolved into having a major focus in online multiplayer gameplay.

The incorporation of online multiplayer gaming has also brought in new commercial elements such as eSports, and the Free-to-play business model into the gaming market, which together contributes to the rapidly growing market of video gaming - the size of the global video gaming industry is estimated to be worth about 159 billion USD in 2020 [2], displaying how the video gaming industry is undoubtedly a massive and profitable one.

1.2 The Video Game Cheating Industry

Many online multiplayer video games share a common element - the emphasis in competition between players. Whether it is a competition for resources (such as in Real-Time-Strategy games like Starcraft 2), a competition to fight for winning a match (such as in round-based shooter games like Counterstrike:Global Offensive), or a literal fight for survival in battle royale games such as PlayerUnknown’s BattleGrounds, players are frequently put together in multiplayer online games to compete with each other, which is a crucial element in making the game engaging and addictive to players.
However, as with other types of games (football, basketball, horse-racing, etc.), with the desire to win against other players, or even the attractiveness of potential tangible rewards (such as reward money from winning eSports competitions), some players will search for ways to cheat in online video games in order to gain an advantage over the others. Targeting the profitability of such a market opportunity, some programmers turn into cheat developers who develop dedicated pieces of software and sell to players at a price to gain an unfair advantage over others. The prevalence of cheating software in modern online video gaming is a major issue that game developers and legitimate players have to deal with daily.

2. Objectives

With the rapid growth of the competitive online gaming market, and inevitably together with the game cheating market, we believe that much of the information related to this topic is not adequately investigated and documented in the academic perspective, as much of the technical information about game cheating is scattered in different underground cheat forums and communities.

Furthermore, due to the inherent nature of “Security through obscurity” in anti-cheat development (Since a public disclosure of anti-cheating techniques is more than certain to allow for cheater developers to pin-point and bypass the exact techniques used in the future), there is even less incentive for anti-cheat developers to publicly release information on the current game cheating and anti-cheating environment.

This project aims to provide academic insight and documentation into the complex and lesser-known domain of game cheating in modern online video games, by laying out the classification of cheats in terms of how they function to obtain an advantage to players, together with a brief overview of common anti-cheat techniques used by game developers, followed by an analysis of
techniques used by cheat developers to bypass existing barriers put in place by anti-cheats.

3. Methodology

3.1 Classification of different existing types of cheats

Modern video game cheats can be classified into 3 main categories in terms of how they exploit the game to gain an advantage for the cheating player, namely:

1. In-Game Exploits
2. Memory Manipulation
   - Internal Cheats
   - External Cheats
     - Usermode
     - Kernelmode
3. Network Manipulation

These categories differ from each other due to their:
- Technical method of exploiting the system
- Difficulty in development and maintenance for the cheat developer
- Difficulty in patching and removing the exploit for the game developer

This section aims to delve into each of the cheat categories and their sub-categories, in order to provide insight into the basic functionality and goals of game cheats in the modern gaming environment from the perspective of a cheat developer.

This section will put a higher focus on analysing memory manipulation cheats, and the advantages they usually offer to cheaters, due to the fact that they are currently the most common and commercially available type of cheating in the market, and is the first priority to defend against for most anti-cheat developers consequentially.
3.2 Overview of common anti-cheat measures

After exploring the topography of video game cheat types from the cheat developer’s perspective, this study will switch over to the game developer and anti-cheat developer’s perspective on the subject, to provide better understanding on how the cheating behaviours in the previous section are commonly detected and reprimanded, mainly focusing on the following topics:

- Client-side Anti-cheating
  - Usermode anticheat
    - Signature scanning and Process Monitoring
  - Kernelmode anticheat
    - Registering callbacks and handle stripping
    - Driver blacklisting
    - Driver Manual Mapping and Detection
- Server-side Anti-cheating
  - Player data analysis
- Game Design and Anti-cheating
  - Memory Encryption
  - Network Encryption
  - Importance of proper data handling in game design

3.3 The future of game cheating and anti-cheating

Lastly, this study will conclude with an overview of the possible future directions that cheat developers and anti-cheat developers may be heading towards, in order to raise their game to defeat each other. Topics covered in this section will include:

- Virtualization technology
  - Direct Memory Access Cheating
  - Cloud Gaming
- Artificial Intelligence
  - Machine learning and cheating detection
- Image Recognition and cheating

4. Schedule and Milestones

- September 2020
  - Project planning and deciding on the scope of the study

- October 2020 - December 2020
  - 4th October 2020
    - Deadline for deliverables of phase 1 (Inception)
    - Detailed project plan
    - Project web page
  - Literature review on game cheat types
  - Memory manipulation cheating code and visual examples
  - Preliminary research into common anti-cheat methods

- January 2021
  - 11-15 Jan 2021
    - First Presentation
  - 24 Jan 2021
    - Deliverables of Phase 2 (Elaboration)
    - Preliminary implementation
    - Detailed interim report

- February 2021 - March 2021
  - Completion of Overview of common anti-cheat methods section
  - Literature review and research on future advancements in cheating and antichecking

- April 2021 - May 2021
  - 18 April 2021
    - Deliverables of Phase 3 (Construction)
    - Finalized tested implementation
Final report
○ 19-23 Apr 2021
- Final presentation
○ 4 May 2021
- Project exhibition

5. References
- [1] Steam Store: Steam Game and Player Statistics
  https://store.steampowered.com/stats/Steam-Game-and-Player-Statistics?l=english