eSports - Professional Cheating in Computer Games

Marc Ruef
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Abstract: Computer game cheating has been around as long as competitive gaming itself. Manipulation is frequently found in the speedrunning scene. Professional eSports and their commercial trappings are making these tricks ever more lucrative. There are various options for gaining an edge in online games. Technical measures can make cheating more difficult or at least detectable after the fact.

Keywords: Artificial Intelligence, Denial of Service, Detect, Drugs, Excel, Exploit, Fraud, Machine Learning, Magazin, Policy

1. Preface

This paper was written in 2018 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20180906* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

2. Introduction

Computer games are big business. Videos, streaming and competitive leagues have driven the commercialization of gaming. However, sponsorships and lucrative prize money also make *eSports* attractive to cheats. This article looks at the current state of cheating in eSports, with insights into bet fixing, doping and technical manipulation.

As long as computer games have been around, players have been trying to break records. Who can get the most points at Pacman or reach the highest level in Donkey Kong? There are numerous traditional records, some of them unbroken for decades and serving as motivation for newcomers to the scene.

2.1. Falsified records

Two of the long-standing titans in this field were Americans Todd Rogers and Billy Mitchell, who held a slew of records which were verified, maintained and publicized by the US-based organization *Twin Galaxies*. When confronted with skeptical inquiries about these records, which had even made it into the *Guinness World Records*, the two men would hit back with brazen arrogance. So the applause was all the louder when their decades of cheating were uncovered in 2018, and they were stripped of their records and titles. Both were banned for life.

Twin Galaxies provides referees and analysts for the purpose of validating records. Over the years, it has become a customary requirement for players to submit video recordings of their own game sessions. Through their contacts, Rogers and Mitchell managed to avoid this validation and chalked up records that in all likelihood were never real.

Todd Rogers held a record of 5.51 seconds for the Atari 2600 game *Dragster*. But when user *Apollo Legend* reverse engineered the game, it became apparent that the purported time was not even possible. The developer of the game *confirmed this* [1] years later. Twin Galaxies annulled the record and *banned Rogers* [2].

Billy Mitchell's downfall came when it came to light that he recorded his record-breaking game for the arcade title *Donkey Kong* using a MAME emulation rather than a printed circuit board (PCB). The user *xelnia* discovered this 35 years later by analyzing the *sequential structure of sprites* [3] in the transition between levels. There are a few key differences between hardware and emulation, meaning that there are also different options for manipulation. All of his records were *removed* [4] by Twin Galaxies and he too was barred.

2.2. Manipulated speedruns

The speedrunner scene is all about pace – the aim is to reach the end of the game as quickly as possible. The player uses any possible shortcuts that the game can offer, ideally without losing a life. These speedruns require an advanced understanding of the game, refined skills and the utmost concentration. If you're a non-speedrunner and think you've got a particular knack for a game, you may well think again when you see what a *professional speedrunner* [5] can do.

The race for the best time can be nerve-wracking and frustrating. This is why players occasionally resort to *splicing*, in which certain sequences are played through until the optimal recording can be achieved. These segments are then put together with an editing program to create the illusion of a perfect speedrun. *Segment runs* are allowed in some games, but they cannot be passed off as *real-time attacks*.

But these edited recordings turned out poorly, especially in the early years. Cheats tended to neglect the *audio track* [6] in particular, which meant manipulation often became evident on closer inspection. Either splices were too rough or cut at the wrong point, or there was unexpected noise on the audio track.

Edits are best carried out during a simple or even static scene, like a loading sequence. But because many games don't have sound for the loading screen, the speedrunning community has focused on the analysis of the image material in recent years. One particularly exciting case is a real-time attack run of the game *Super Meat Boy* from 2012. The user *ExoSDA* was caught red-handed because the *bandage girl autosave animation* has a particular rhythm that has to remain consistent across different loading sequences. By *analyzing it frame by frame* [7], it became apparent that the segments from different runs had been spliced together:

> *At 60 FPS, her arms move in a regular 40-frame cycle, so her arms will be up for 20 frames and then down for 20 frames. At 30 FPS, these values are halved, so we would expect a 20-frame cycle with 10 frames of arms up and 10 frames of arms down. Rinse and repeat.*

Those discovered manipulating the results in this way are stripped of their records and lose their standing among their gaming peers. For anyone deeply involved in the scene, this is no doubt a major blow. But for the independent observer such cases seem more like trivial bickering.

3. Professional eSports

The first officially documented computer game competition took place in 1972 at Stanford University, where enthusiasts played the classic game *Spacewar* for the prize of an annual subscription to *Rolling Stone* magazine.

Almost 50 years later, the *eSports* competitive computer game scene has become thoroughly professionalized. Now individual players or teams compete against each other. Typically this will involve games in the genres of *real-time strategy* (RTS), *first-person shooter* (FPS), *fight games* and *multiplayer online battle arena* (MOBA).

This professionalization has been driven by economic factors, with players now competing for prestigious, highly lucrative *prizes*. And well-known players have further opportunities for monetization with *sponsoring and advertising deals*. But for this to happen, competitions have to be held on the Internet and on *broadcast live* on TV stations. In 2015, there were 226 million viewers, with the eSports sector generating USD 325 million. The following year, revenues hit *USD 493 million* [8], and there is still a strong upward trend.

Cheating may have become a major issue once the sector started pulling in the big bucks, but it has been around for quite some time. It's just that now that the stakes are higher, cheats are getting far more sophisticated in their methods. They are spending more and investing more heavily in manipulating the outcome of games.

3.1. Manipulated betting

Much like traditional sports, the eSports sector allows *betting* [9]. Well-known betting outfits have specific areas on their sites for eSports. Typically they offer the options of *winner/loser* and *score ratios*, but major betting companies also allow game-specific and exotic or highly dynamic bets, such as *first kills* or *even/odd kills*.

Here, too, odds are calculated and offered, and betters can use them to decide where to place their wagers. *Betting fraud* makes it possible to force wins. This could involve *collusion* with one or more participants in a competition. *Match fixing* involves deciding who will lose (and consequently who will win). This kind of *cheating to lose* is very easy to implement and can even work without the cooperation of other players or referees (meaning only one party is involved).

On the one hand, manipulated betting may be discovered during the game itself, for example, when observers notice atypical gaming behavior, such as players performing below their normal, expected level. Computer-aided analysis, particularly when it is combined with artificial intelligence, can be used to detect unexpected behavior.

On the other hand, *analysis of betting behavior* [10] can turn up signs that point to manipulation. Here, too, the aim is to detect anomalies. These might include a large number of bets placed at the same time, unusually large wagers or betting *against the statistical odds* [11]. Among the well-documented examples are bets for games like *StarCraft* [12], *Counter-Strike* [13] and *League of Legends* [14]. Data correlations can uncover fraud networks and determine who is running the racket or who is involved.

3.2. Doping, drugs and stimulants

Doping is traditionally associated with strength and endurance sports, such as weightlifting and cycling. But there are other sports that *are prone to drug use* [15], particularly those with a disproportionate emphasis on mental performance. And eSports are *no exception* [16].

In recent years, various active and now inactive players have *confessed* [17] to taking performance-enhancing drugs, either on their own initiative or at the behest of their coach. The *Electronic Sports League* (ESL) has *collaborated* [18] with the *World Anti-Doping Agency* to draw up a *List of Prohibited Substances* [19]. The following are particular favorites among players, *including those on the poker circuit* [20]:

- Adderall
- Modafinil
- Donepezil
- Propranolol

These promise to enhance:

- Learning
- Memory
- Alertness

- Concentration
- Reaction times
- Motor skills
- Strength
- Better ability to respond to negative outcomes (e.g. losing)

Anyone who consumes marijuana for medical reasons, for instance, must *disclose this in advance* [21] and provide a doctor's certificate.

Originally, there were plans for skin tests for prohibited substances, but testers decided on saliva samples for practical reasons. These are collected during the competition without warning. In contrast to sports such as football and tennis, there are (currently) no plans for tests outside of competitions.

3.3. "Whispering"

One means of cheating that is very simple in theory is *"whispering"* or passing on information. In competitive games, a player gains an advantage if they become privy to unknown information at an early stage. That could include information about an opponent's position or allocation of resources.

This kind of knowledge can be passed on by members of a team communicating information to each other. This could come from seeing this information on a screen (screen peek), which happened with the *Azubu Frost* team *during the 2012 World Championship* [22] of *League of Legends*. Or a player might gain additional information about what is currently happening in the game after being eliminated (e.g. spectator mode).

On the other hand, information can be passed on by non-players, including spectators. Indirectly, this category of course also includes the overall behavior of the audience, which might greet moves or decisions with a murmur or a roar. But actors in the audience may also want to deliberately pass on information to players. This could include concrete examples of calling out information or instructions, or coded messages such as *coughing* [23] as seen in the British version of *Who Wants to Be a Millionaire?*.

Information can also be passed on with technology, such as team members giving extra instructions through headsets. Manipulated headsets can be used to transmit instructions via radio, thus avoiding monitored communications through computers and networks.

Various measures are used to counter this form of external influence. Players often have to wear *heavy-duty ear protection*, and their headsets may additionally be fitted with *white noise* or *noise-canceling* functions to prevent undesirable communications.

3.4. Technical cheating

So far, our look at cheating has concentrated largely on non-technical methods. But technical cheating is a huge factor in eSports, so let's take a closer look at the various options for cheating at the technical level.

3.4.1. Breaking in-game rules

In contrast to manipulated betting, technical cheating is all about *cheating to win*. By breaking in-game rules, players attempt to exploit the idiosyncrasies of the game's mechanics. These include:

- bugs
- glitches
- skips
- exploits

These idiosyncrasies are often *exploited during speedruns* [24] to set practically impossible records. For example, in *Bioshock* there is a *skip glitch* [25] which can shave several minutes off a player's time. But here, too, there is *ongoing discussion* [26] about the validity of speedruns with glitches. Some argue that they are part of the program and therefore fair game for exploitation. Developers of *Pokémon Gen 1*, for instance, incorrectly implemented the *Poké Doll* object, which can provide a decisive advantage in the fight against the *Marowak Ghost*. The titles in the classic Metroid series are deliberately based on non-linear possibilities in the gaming environment. Others call for a clear distinction between speedruns with glitches and those without ("glitchless" or "no skips").

But over time a hybrid status has emerged for certain games. In some difficult passages, such as those that depend on the time elements of *luck and chance* [27], skips and exploits are permitted (in Zelda and Fallout, for instance).

The classic example of an exploit in competitive eSports is the design flaw in the *Overpass* map in *CS:GO*. When one player climbed on top of another, they could *view the map* [28]. This inevitably provided a tactical advantage. Using this *boost* led to the *disqualification* [29] of the well-known *Fnatic* team in 2017.

Another example in competitive eSports was a *wall glitch* [30] in *PlayerUnknown's Battlegrounds* (PUBG), which was consistently and successfully exploited at the 2018 IEM event in Poland. There was no less than USD 50,000 in prize money at stake, so there was considerable outcry from gamers. These errors are one reason why the *FIFA game series* [31] is yet to find a lasting place in commercial eSports.

It is up to the developers of the games to recognize these exploits and correct them with patches. This is the only way to guarantee a stable platform that prevents players gaining an underhand advantage. But it's not as easy as it sounds. Many developers are simply not interested in creating the perfect eSports game. Some studios, for instance, discontinue support for their games after a certain time, so it's up to the competitive scene to define what is and isn't permitted. Sometimes the matter is even resolved with a custom patch.

3.4.2. Software hacks

Software hacks are particularly popular in competitive online gaming at the amateur level. Here an existing game is manipulated or expanded to provide advantage for the player.

One very simple method that some online gamers have had to contend with is the *disconnect* (abort game), which is when a player who is about to lose a game simply disconnects their system. In the case of many titles, the game isn't counted and the lost points and lost game aren't factored into the statistics. Developers can counter this by continuing to allow reconnects (for a certain time), by counting canceled games, or slapping a temporary ban on anyone with a suspicious number of disconnects to their name.

A similar approach is to use a local *lag switch* [32] or (temporary) *denial of service attack* (DoS) to restrict an opponent's network access through flooding. But this can also allow a player to deliberately direct the flow of the game by forcing a slow-motion effect or using arrhythmic movements (lagging).

Rapid fire has been used in video game consoles since the early days. In certain games where players have to shoot laboriously and repeatedly, a turbo button can automate this mechanical process. This prevents fatigue and under certain circumstances can reach a constant frequency that cannot be achieved through natural means.

Triggerbots are often used to enable shooters to force automatic firing as soon an opponent is fixed in the cross-hairs. This can save valuable time between recognizing the opponent, aiming and firing, because the player merely has to aim to force the required hit within a fraction of a second. This non-human response time can be statistically proven, which is why advanced bots try to evade detection through artificial delay.

Aimbots [33], also known as *auto-aim*, go one step further by taking care of the aiming as well. This usually happens at the code level, so it has no impact on the controls and therefore the direct gaming experience of the player. Aimbots can be detected through statistical information. In particular, the timing between identification of a target, aiming, and firing is consistently short and thus highly conspicuous (even more so than triggerbots).

With a *wallhack*, which can be excellently combined with aimbots, players can see or even shoot through walls (even if the physics of the game don't allow it). Most implementations work by displaying the outline of the opponent behind the wall (x-ray view). This enables early detection of the number, position and movements of opponents, offering an anticipatory advantage.

One indirect option is *extra-sensory perception* (ESP), which involves modifying a game with additional mechanisms to pass on information to the player. This might include a joypad that vibrates on approach of opponents, even before they become visible. This approach is harder to detect as an anomaly in a game, as all ESP usually does is provide additional data; the player still has to respond to it, however. At first glance, the behavior may seem highly organic.

With round-based games, *look-ahead* can offer an advantage. This approach is particularly favored for strategy and card games where the player has to wait for other players to act before they can select and communicate their own move. A lockstep protocol can hinder this approach.

In his talk, John McDonald explains how *Valve* uses *machine learning* to identify and neutralize cheats based on their *behavioral patterns*. The *Valve Anti-Cheat* system (VAC) offers a promising approach and one that is urgently required if competitive (online) games are to remain appealing to legitimate players in the future.

3.4.3. Hardware hacks

In addition to the usual software hacks, there are also hardware hacks. These involve manipulating hardware to enhance and optimize functionality. Existing hardware may be modified or additional components added. The simplicity and accessibility of *Arduino* makes it a popular option.

Mechanical, computer-aided control of hardware is also an option in some cases. Joypads and phones, for instance, can be linked up in certain configurations so that they trigger mechanical input, although at present this is largely a trick carried out by hobbyists who still see it as being in the proof-of-concept phase.

In some tournaments, particularly in the lower leagues, players sometimes smuggle in *built-in USB devices*. These are illicit USB devices that are installed into legitimate components. A player may bring a hardware mouse, for instance, which additionally conceals a USB memory device. This might be a USB hub and a '*BadUSB*' (e.g Rubber Ducky or Teensy).

This can be automatically opened by the operating system to offer expanded functionality as a *cheat injector*. Other methods hide the cheat code in the *drivers of the hardware components*, making them very difficult to detect.

These include hardware-based *triggerbots* [34]. The demo videos of these triggerbots are contentious, as the functionality shown cannot be achieved solely through the hardware used. But the combination of different sensors and automatisms is certainly conceivable.

4. Conclusion

Cheating at games is probably as old as humanity itself. Competitive games, particularly where financial reward is involved, are of course particularly attractive targets.

And eSports are no exception. In addition to the classic methods of collusion, bet fixing and performance-enhancing substances, there may be various technical methods in play. By exploiting the idiosyncrasies of a game, players can gain an advantage just as they can by manipulating software and/or hardware.

Game developers, leagues and referees are all concerned with preventing, hampering or at least detecting this kind of fraud. The more money that is invested in eSports, the more effort goes into thwarting undesirable cheats – an interdisciplinary task that comes with plenty of challenges.

5. External Links

[1] https://www.twingalaxies.com/feed_details.php/87/dragster-designer-without-a-shadow-of-a-doubt-about-todd-rogers-record
[2] https://www.twingalaxies.com/feed_details.php/104/twin-galaxies-dragster-dispute-concludes-with-banning-of-todd-rogers/5
[3] http://donkeykongforum.com/index.php?topic=2055.msg33395#msg33395
[4] https://www.twingalaxies.com/feed_details.php/1047/billy-mitchells-donkey-kong-and-all-other-records-removed/4
[5] https://www.youtube-nocookie.com/watch?v=E8xXtoIm76s
[6] http://blog.tobiasrevell.com/2018/04/speedrunning-or-playing-playing-game.html
[7] https://docs.google.com/document/d/1YWiHvjJf96LEz95BJFPmW7NZJxg-0awDCWgLoGrgK_U/edit
[8] https://newzoo.com/resources/
[9] https://compete.kotaku.com/how-esports-gambling-works-1823959797
[10] https://www.thelines.com/esic-esports-betting-fraud-detection/
[11] https://compete.kotaku.com/starcraft-remastered-pro-arrested-for-match-fixing-1823809648
[12] https://compete.kotaku.com/starcraft-remastered-pro-arrested-for-match-fixing-1823809648
[13] https://compete.kotaku.com/esl-lifts-lifetime-ban-on-counter-strike-match-fixers-1797190447
[14] https://kotaku.com/league-of-legends-pro-attempted-suicide-after-tournamen-1542880793
[15] https://en.chessbase.com/post/brainpower-drugs-doping-in-che
[16] https://www.businessinsider.com/esl-drug-testing-for-adderall-2015-7
[17] https://www.youtube-nocookie.com/watch?v=0VK6nkA__hc
[18] https://www.theverge.com/2015/8/12/9143819/e-sports-banned-drugs
[19] http://list.wada-ama.org/
[20] https://www.casino.org/blog/ritalin-use-in-poker-esports/
[21] https://www.reddit.com/r/GlobalOffensive/comments/3gmog8/esl_announces_details_of_the_antidoping_policy/
[22] https://www.pcgamer.com/riot-rules-on-league-of-legends-screen-watching-incident-issues-30000-fine/
[23] https://www.youtube-nocookie.com/watch?v=bQoNWw0G2AY
[24] https://kotaku.com/why-speedruners-use-glitches-1582919382
[25] https://www.youtube-nocookie.com/watch?v=Ny3whooBTWI
[26] https://www.reddit.com/r/speedrun/comments/7mfdes/why_are_exploits_allowed_in_speedruns/
[27] https://www.youtube-nocookie.com/watch?v=SnQNrYOvWR4
[28] https://www.youtube-nocookie.com/watch?v=cNQ71mfmt80
[29] https://kotaku.com/cheating-fiasco-leads-to-incredible-counter-strike-fina-1665293838
[30] https://twitter.com/TSMViss/status/968254478666424322
[31] http://www.esports-news.co.uk/2017/11/18/fifa-glitches-esports/
[32] http://compnetworking.about.com/od/consumerelectronicsnetworks/f/lag_switches.htm
[33] https://www.wired.com/gaming/virtualworlds/commentary/games/2007/04/gamesfrontiers_0423
[34] https://www.youtube-nocookie.com/watch?v=NMTqQe3vv3k