Ravi Nayyar (ravin)

Ben Prikle (bpirkle)

Game Security Resource Proposal

**Realtime Detection of Hardware Spoofing Mechanisms to Prevent Activision User Cheating**

Activision has seen a sharp increase in the number of users who actively use cheats (or hacks) in multiplayer first person shooter (FPS) games over the last few years. Flagship FPS games like Call of Duty COD Warzone have had nearly 500,000 permanent bans since its inception (Staff). Though some banned account users have claimed that they themselves were hacked, the sheer number of banned users has made it clear that the current steps being taken are not solving the problem.

Cheats like aimbots which automate the process of finding an enemy player or wallhacks which allow the user to see enemies hidden by walls or barriers have become so widespread that game ecosystems are suffering. Warzone in particular has seen high profile player loss and the refusal to join tournaments due to the pervasive use of cheats (Bicchierai).

Activision has taken steps to curtail the implementation of cheats used by a subsection of their player base from facilitating the ease of which cheaters are reported to issuing hardware bans which prevent users from simply playing with another smurf[[1]](#footnote-1) account on the same machine (Staff). However, more concrete steps need to be taken to automatically detect and then report those who use cheats.

With aim related hacks being the some of the popular and detrimental form of cheating, the goal of our research team is to create a system to detect, at a certain level of probability, whenever a player is using the aforementioned forms of automation and react accordingly based on Activison’s policies. We will first conduct research on the different versions of aim assist hacks that exist – how they differ in functionality and what common methodologies they all employ. Then, we will start the development of a rudimentary Aim-Assist Cheat Detection System (ACDS). The ACDS will be iteratively built – first focusing on aimbots then anti-recoil cheats, etc.

Regarding the evaluation of our work, the system will be continually tested against commercially available and currently deployed cheats. Our measure of success will be determined not only by if the systems is able to detect cheats, but also at the rate it is able to do so. With the end goal being preventing cheating during multiplayer sessions, the faster a cheaters account is banned, the greater the chance that reputable users will continue playing the game. Our deliverable will consist of the ACDS as well data showing its efficiency against commonly used game hacks.

The project will be completed in the 2021-2022 academic school year. 12 credits will be allocated in the Fall (due to other courses also being taken) and 24 credits will be allocated in the spring. The first half of the year will revolve around conducting research on current cheating and anti-cheating methodologies and preliminary development on the ACDS while the second half will focus on ACDS construction and testing as well as a final project report.

Citations

Bicchierai, Lorenzo Franceschi. “'Warzone' Streamers Are Quitting the Game Because of Cheating Wave.” *VICE*, www.vice.com/en/article/qj8nnm/warzone-streamers-are-quitting-the-game-because-of-cheating-wave.

Staff, Call of Duty. “An Update - Call of Duty Anti-Cheat Progress Report.” *An Update - Call of Duty Anti-Cheat Progress Report*, www.callofduty.com/blog/2021/04/warzone-anti-cheat-progress-report.

1. A smurf account is a non-primary account that allows players to interact with other users while hiding their proficiency at the game or to take some action that they do want their main account to be associated with. [↑](#footnote-ref-1)