Computer scientists launch counteroffensive against video game cheaters

November 16 2020

Credit: Pixabay/CC0 Public Domain

University of Texas at Dallas computer scientists have devised a new weapon against video game players who cheat.

The researchers developed their approach for detecting cheaters using the popular first-person shooter game Counter-Strike. But the mechanism can work for any massively multiplayer online (MMO) game that sends data traffic to a central server.

Their research was published online Aug. 3 in *IEEE Transactions on Dependable and Secure Computing*.

Counter-Strike is a series of games in which players work in teams to counter terrorists by securing plant locations, defusing bombs and rescuing hostages. Players can earn in-game currency to buy more powerful weapons, which is a key to success. Various software cheats for the game are available online.

"Sometimes when you're playing against players who use cheats you can tell, but sometimes it may not be evident," said Md Shihabul Islam, a UT Dallas computer science doctoral student in the Erik Jonsson School of Engineering and Computer Science and lead author of the study, who plays Counter-Strike for fun. "It's not fair to the other players."

In addition to fair play, cheating also can have an economic impact when dissatisfied players leave to play other games, Islam said.

Cheating incidents also can have serious consequences in esports, a fast-growing industry with annual revenues close to $1 billion. Cheating can result in sanctions against teams and players, including disqualification, forfeiture of prize money and a ban on future participation, according to the Esports Integrity Commission based in the United Kingdom.

Detecting cheating in MMO games can be challenging because the data that goes from a player's computer to the game server is encrypted. Previous research has relied on decrypted game logs to detect cheating after the fact. The UT Dallas researchers' approach eliminates the need for decrypted data and instead analyzes encrypted data traffic to and from the server in real time.

"Players who cheat send traffic in a different way," said Dr. Latifur Khan, an author of the study, professor of computer science and director of the Big Data Analytics and Management Lab at UT Dallas. "We're trying to capture those characteristics."

For the study, 20 students in the UT Dallas class Cyber Security Essentials for Practitioners downloaded Counter-Strike and three software cheats: an aimbot, which automatically targets an opponent; a speed hack, which allows the player to move faster; and a wallhack, which makes walls transparent so players can easily see their opponent. The researchers set up a server dedicated to the project so the students' activity would not disrupt other online players.

The researchers analyzed game traffic to and from the dedicated server. Data travels in packets, or bundles, of information. The packets can be different sizes, depending on the contents. Researchers analyzed features, including the number of incoming and outgoing packets, their size, the time they were transmitted, their direction and the number of packets in a burst, which is a group of consecutive packets.

By monitoring the data traffic from the student players, researchers identified patterns that indicated cheating. They then used that information to train a machine-learning model, a form of artificial intelligence, to predict cheating based on patterns and features in the game data.

The researchers adjusted their statistical model, based on a small set of gamers, to work for larger populations. Part of the cheat-detection mechanism involves sending the data traffic to a graphics processing unit, which is a parallel server, to make the process faster and take the workload off the main server's central processing unit.

The researchers plan to extend their work to create an approach for games that do not use a client-server architecture and to make the detection mechanism more secure. Islam said gaming companies could use the UT Dallas technique with their own data to train gaming software to detect cheating. If cheating is detected, the system could take immediate action.

"After detection," Khan said, "we can give a warning and gracefully kick the player out if they continue with the cheating during a fixed time interval.

"Our aim is to ensure that games like Counter-Strike remain fun and fair for all players."

More information: Md Shihabul Islam et al. GCI: A GPU Based Transfer Learning Approach for Detecting Cheats of Computer Game, *IEEE Transactions on Dependable and Secure Computing* (2020). DOI: 10.1109/TDSC.2020.3013817

Provided by University of Texas at Dallas

Citation: Computer scientists launch counteroffensive against video game cheaters (2020, November 16) retrieved 25 April 2024 from https://techxplore.com/news/2020-11-scientists-counteroffensive-video-game-cheaters.html