Analyzing the Arms Race between Anti-Cheat Developers and Cheat Developers

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science in Computer Science

Thai-Phuc Nguyen

Spring, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____Thai-Phuc Nguyen_____

ADVISOR

S. Travis Elliott, Department of Engineering and Society

Analyzing the Arms Race between Anti-Cheat Developers and Cheat Developers

As video game anti-cheat systems improve, their corresponding cheat programs also continue to develop, constantly trying to find a weakness and exploit it. This "arms race" between anti-cheat and cheat developers mainly stems from the monetary incentives and demands for cheats provided by cheating players, forcing video game developers to be in a constant battle with cheat programs in order to protect the integrity of the game (Russo, 2020). Even if the technical solution – completely changing the gaming system environment to prevent cheats from even being installed – works, there is still a concern that cheat developers will continue trying to breach that security and develop a new type of cheat programs for this new environment. As long as cheat developers are incentivized by cheating players' demands, it will only be a matter of time before the band-aid of anti-cheat is ripped off. (Lehtonen, 2020, p.67). Considering gaming is a multi-billion dollar industry and that is just looking at the online multiplayer game market according to Irdeto in 2018, minimizing cheating to protect the integrity of games becomes a huge monetary incentive for video game companies.

The goal of this paper is to propose a starting point towards the process of completely eliminating this costly arms race. Through the usage of analogies between anti-cheat technology arms race and military technology arms race, there are parallels with the military technology arms race that will show that video game companies should start looking at the root of the problems: the cheating players and why they want to cheat in the first place. Further looking into the incentives of cheating for players might reveal a new method that reduces those incentives, instead of simply limiting different ways that they can fulfill those incentives (Chen & Ong, 2018, p.276).

Background: Kernel and User Modes

For a brief technical explanation, there are two main levels or modes for an operating system to run a program: user mode and kernel mode. As seen in figure 1 below, the kernel mode is at ring 0 which means that the program running would have the most privileges, giving unrestricted access to the CPU and memory, as opposed to a program being run in user mode at ring 3 which needs to request access to a specific hardware or memory resource.

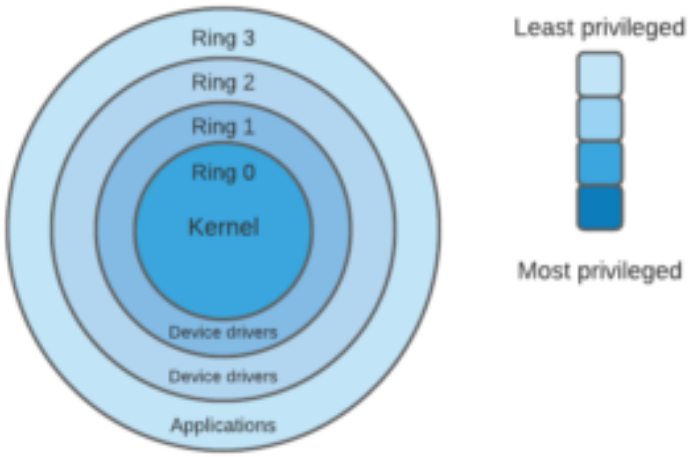

Figure 1: Operating system protection rings are the most common implementation to separate kernel level at ring 0 and user level at ring 3 (Baeldung, 2021)

In simpler terms, programs at the kernel level have full access and therefore control of the entire computer system, both hardware and software, which obviously is considered an extreme security risk.

Defining the Nature of the Anti-Cheat Technological Arms Race

First, the basis of this technological arms race are rather obvious, financial incentives. Anti-cheat developers are paid by the gaming company because fewer cheats being abused in a game would mean more players enjoy that game and therefore a higher profit. The better a game

does financially, the more benefits the anti-cheat developers of that game receive. Similarly, the cheat developers are also incentivized to continue the arms race for a financial reward. To be in fact, cheat development has become something like a market, a monthly subscription business where players pay in order to gain access to and use cheat programs that can sneak past the current anti-cheat system (Russo, 2020). There are some nuances to consider. There are other incentives for cheat developers that do not stem from monetary gains. A major example of this is from Russo's interview with a cheat developer whose motivation is the same as someone who wants to crack the code and solve a puzzle, simply looking to overcome a challenge. While this adds more to the already unbalanced fight between anti-cheat and cheat developers, these cheat developers with different motives do not mean to cause harm to the companies and could be recruited to help identify weaknesses in the current anti-cheat system.

Now, the nature of this arms race is actually a one-sided battle of the limited anti-cheat developers against the large and anonymous cheat developers. If nothing of significance is done to this continuously losing battle against cheat developers, the online multiplayer gaming market will constantly be bleeding money and losing profit. This is a rather costly but necessary investment for the video game companies. As stated before, the online multiplayer gaming market was estimated to be 116 billion dollars in 2018. Yet with the presence of cheating, there is an estimated 77% reduction of the potential player base or consumers of this multi-billion-dollar market. Additionally, almost half of surveyed gamers state that they would not purchase in-game content, which is a major portion of profit for a lot of games, especially if they are free (Irdeto, 2018, p.2-3). Anti-cheat developers are at a constant disadvantage, always fighting an uphill battle. First of all, there are simply more cheat developers trying to break in than anti-cheat developers protecting the system. This is due to the fact that cheat developers can come from

anywhere in the world with internet access and can also remain completely anonymous online. But, the biggest problem anti-cheat developers face is a fight at the kernel level, where programs basically have complete control of a computer. On one hand, cheat programs are run by a small percentage of players who are willing to risk the consequences. This means that cheat players can install cheats at the kernel level, even going as far as prioritizing the cheat programs over the startup of their own operating systems, in order to avoid detection by anti-cheat (Li, 2021). The only way to combat a kernel level threat is for anti-cheat developers to install their software at the kernel level as well. However, on the other hand, anti-cheat systems are applied to every single player, where not everyone wants to be subjected to an intrusive anti-cheat at the kernel level. This would result in potential player base backlash if anti-cheat developers attempt to fight fire with fire (Rasidi, 2020). This becomes a delicate balancing act for the anti-cheat developers, treading the sensitive line between customer security and the integrity of the game.

An example of this would be the development of modern competitive shooter games like Valorant. The first-person shooter gaming scene has been heavily plagued with cheatings from blatant to seemingly undetected. Riot Games, the company responsible for the development of Valorant, focuses heavily on an intrusive anti-cheat system that would shutdown all common methods of cheatings called Vanguard (Rasidi, 2020). This brought up a lot of controversies as Vanguard was an extremely intrusive system, working on the same level of the operating system of many computers. While it has undoubtedly significantly decreased the amount of cheating seen in Valorant, this delicate security balance relies entirely on Riot Games and their security, both literal and moral. The weakest link is one bad apple in the company deciding to exploit all of this available data and causing a data breach with access to the operating system of hundreds of thousands of personal computers.

Understanding the Temptations and Incentives of Online Cheating

It is of interest for the online multiplayer gaming market to eliminate this continuous and costly arms race. Returning to the root cause of the problem, understanding the reasons why players want to cheat and what possible actors can influence those incentives, which could lead to a different approach in lowering cheats in video games.

Starting at the beginning, the definition of cheating is rather subjective and was outlined by Chen & Ong (2018) with 5 different behavioral schemas: "intentionality", "utility", "core gaming goals", "evolving gaming norms", and "social ties to gaming communities". Not only do these serve as ways players define cheating, but also reasons players justify cheating. First, "intentionality" means that a behavior is acceptable if "said action is 'caused' by the game designer" (pg. 277). This means exploiting glitches or loopholes in the code of the game is not considered cheating. Second, "utility" means that a behavior is unacceptable if it is used for self-benefit over the game community, like cheating to get an advantage over non-cheating players. Similarly, "core gaming goals" means that a behavior that prevents players from "achieving their core gaming goals" is not acceptable (pg. 279), like getting an advantage over non-cheating players which would create an unfair/unbalanced playing field. Next, "evolving gaming norms" means that cheating becomes normalized after existing in a game for a long time. This is especially true for games that are no longer being supported by their developers and therefore allowing the player base to redefine the "norms" of how a game is played however they want. Lastly, "social ties to gaming communities" focuses on players who cheat because they are surrounded by other players who cheat, normalizing something that shouldn't be normalized and allowing them to ignore the ostracisation of non-cheating players (pg. 280-281). This reveals one actor that influences players' incentives to cheat is social ties/connections with other cheating

players, which also explains why one of the best ways to prevent cheating is to not inform players that a cheat exists, cutting connections with any cheating parties. Even personality traits can be considered as another actor that affect people's incentives to cheat, not just in video games (Karim, Zamzuri, & Nor, 2018, p.91). It is shown that people with a high level of conscientiousness would be less likely to commit fraudulence, plagiarism, and misuse. On the other hand, extraversion has a slightly higher chance of resulting in potential unethical internet behaviors. It is important to try and map out as many actors as possible to find connections and relationships with players' incentives to cheat.

Intellectual Framework Background

Based on the article "The Power of Analogies for Imagining and Governing Emerging Technologies" by Schwarz-Plaschg**,** I can use analogical imagination as a mode of deliberation for understanding the impact of emerging technologies, which in this case is about the anti-cheat technological arms race. I will adapt this framework but with the concepts or the history of the military arms and space race during the Cold War instead of just technology, find connections between existing "technology" with my own STS topic of the arms race between anti-cheat and cheat developers. The framework strives to help people understand new and difficult technological concepts by relating it to existing concepts that they have already been exposed to.

The strength of this intellectual framework lies in the creation of analogies providing innovative perspectives on issues, rather than re-creating known information. "Despite the fact that various technologies are never tailor-made analogical sources for new technologies, they can still supply important learning experiences that can be used for enhancing anticipatory capacities, especially with regard to governance processes." (Schwarz-Plaschg, 2018, pg.4-5). Creating multiple analogies addresses different components and allows for an understanding of more than

one dimension of the problem. However, the weaknesses of this framework lie in limitations of analogies and "framing effects". This framework does not allow for exploration of extremes future scenarios, as analogies need to focus on realistic past examples in order to draw from valuable lessons. Furthermore, analogies may provide a "framing effect", where it gives a specific understanding of reality and shielding against counter-arguments. In other words, if used wrong, analogies can cause tunnel visioning on the specificity of a reality, preventing one from fully seeing the bigger picture.

The Analogies Between the Anti-Cheat Technology Arms Race and the Military Technology Arms Race

The arms race between anti-cheat and cheat developers has a lot of similarities with the historical military arms and space race between the Russian and United States during the Cold War period. At first glance, the arms race between anti-cheat and cheat developers is rather "action-reaction", where a new cheat program is put out, which would lead to anti-cheat being updated to cover this weakness, which would lead to a new cheat program being developed, and the cycle continues. However, diving further reveals that there's actually an external actor in this arms race that is causing this back-and-forth nature. This, of course, being the demands from cheating players or players that want to cheat. Similarly, in the military, specifically nuclear, arms race during the Cold War, Trachtenberg et al. actually revealed that the Cold War arms race was not a "US-led action-reaction arms race", but there was a lot of inaction in response to an action of the opposing side, and vice versa. (2021, pg.550-552). In fact, the US reacted defensively in response to a lot of the Soviet Union's expansion, similarly to anti-cheat developers responding to the constant development of cheat programs. There is a difference between these 2 arms races: the external actor of players wanting to cheat creates a new dynamic

that continues to push the cheat developers to continue expanding. In the nuclear arms race, the situation diffused naturally after enough deterrence was developed on both sides which led to the signing of multiple arms control treaties. However, in the anti-cheat technological arms race, there will never be enough deterrence to diffuse the situation naturally. The cheating players act as an external force that constantly pushes the arm races forward.

This analogy allows for better understanding of the anti-cheat arms race utilizing history. But, even more importantly, the difference between these two situations shows that if the external actor of the cheating players can be removed from the system, there is a way to naturally diffuse the arms race. With the insight gained from the analogy matching with the insight gained from problem framing my own STS research topic, this further emphasizes the importance of understanding and then, reducing the incentives for players to cheat in video games. This would, of course, be a major step towards ending the arms race and reducing cheating in video games.

Conclusion

The research question that this seeks to answer is how effective a solution is addressing the incentives of online cheating in order to eliminate the arms race that is plaguing the online multiplayer gaming market? And this would clearly benefit the online multiplayer gaming market, specifically all of the different video game companies and developers who are seeking to escape the constant draining of profit from this arms race and reduce cheating in their games. Subsequently, this would benefit the gaming community as a whole as the player base's enjoyment of online multiplayer games would increase as cheating decreases.

Works Cited

- Baeldung. (2021, June 23). What's the Difference Between User and Kernel Modes? *Baeldung on CS*. https://www.baeldung.com/cs

- Chen, V. & Ong, J. (2018) The rationalization process of online game cheating behaviors, Information, Communication & Society, 21:2, 273-287, DOI: 10.1080/1369118X.2016.1271898

- Irdeto (2018). *Irdeto Global Gaming Survey: The Last Checkpoint for Cheating* [Data set]. Irdeto. https://resources.irdeto.com/irdeto-global-gaming-survey

- Karim, N., Zamzuri, N. & Nor, Y. (2009, August) Exploring the relationship between Internet ethics in university students and the big five model of personality, Computers and Education, 53:1, 86-93, DOI: 10.1016/j.compedu.2009.01.001

- Lehtonen, Samuli (2020). Comparative Study of Anti-cheat Methods in Video Games [Master's Thesis, University of Helsinki]. Digital Repository of the University of Helsinki.

- Li, Victor (2021, May 30). The Anti-Cheat Arms Race: Why developers can't seem to beat cheaters. *SuperJump*. https://superjumpmagazine.com

- Rasidi, Sidharta. (2020, October 8). Why You Should Be Wary of Kernel-Level Anti-Cheat. *KeenGamer*. https://www.keengamer.com

- Russo, Jimmy (2020, August 4). A game of chess: an interview with a Fortnite cheat developer. *Fortnite Intel*. https://fortniteintel.com

- Schwarz-Plaschg, Claudia (2018). The Power of Analogies for Imagining and Governing Emerging Technologies, NanoEthics, 12, 139-153, DOI: 10.1007/s11569-018-0315-z

- Tranchtenberg, D., Dodge, M., & Payne, K. (2021). The “Action-Reaction” Arms Race Narrative vs. Historical Realities, Comparative Strategy, 40:6, 521-562, DOI: 10.1080/01495933.2021.1983336