**Transition from Client-Sided to Server-Sided Gaming Systems**

(Technical Topic)

**Understanding the Temptations and Incentives of Online Cheating**

(STS Topic)

**A Thesis Project Prospectus in STS 4500 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

Fall, 2021

Technical Project Team Member(s):

Thai-Phuc Nguyen

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_____

ADVISORS

Kathryn A. Neeley, Department of Engineering and Society

Daniel Graham, Department of Computer Science

**Decreasing the Presence of Cheating in Online Multiplayer Video Games without Compromising User Security**

Cheating has been present in video games since the start of single-player console games (McFerran, 2016). This would later spread to multiplayer games as well, which led to the first anti-cheat, which is the introduction of real-time scanning for cheat programs in order to ban cheaters (Lehtonen, 2020, p.6). This becomes an arms race, a chess game between anti-cheat and cheat developers (Russo, 2020). Anti-cheat software has developed considerably over the years, but it has a limitation of only being able to detect programs it has accessed. On the other hand, cheat programs are not limited by this since they are willingly installed by the users. This means that the users can always allow the cheat programs to be more invasive and start up earlier than the anti-cheat. Unlike the willingness of a few that utilize cheats, an invasive anti-cheat system would need to be installed for the whole playerbase, in which not many are willing to sacrifice their security. This raises a question of whether it is necessary to switch to a server-sided game environment in order to stop this rather one-sided arms race between anti-cheat and cheat developers.

Without any anti-cheats or other measures against cheatings, over thousands to hundreds of millions of dollars would be lost by game companies (Lehtonen, 2020, p.5). As mentioned above, for the technical topic, I will determine whether or not a transition from client-side to server-side in terms of a game environment will be feasible to address this one-sided arms race. Moreover, I will research and learn more about what drives people, specifically gamers, to cheat in video games to the point that they are willing to purchase subscriptions for these cheats, encouraging the development of more cheats, as part of this project's STS topic. Through a better

comprehension of why cheating is a prominent problem, a potential psychological solution could be found to decrease the reasons why cheating in video games happens in the first place.

**Transition from Client-Sided to Server-Sided Gaming Systems**

First to understand the nuances of anti-cheat systems, an understanding of the protection rings of a computer is necessary. Kernel-level provides access to a whole computer while user-level needs permissions to access hardware and memory (Baeldung, 2021). This leads to a lot of public concern towards the implementation of kernel-level anti-cheat systems that have almost full access to a player's computer (Rasidi, 2020).

Current games are client-sided which means that the games are on the players' computers and all of their inputs are local. For multiplayer games, these would be transferred to a server but most of the player's interaction with the game is local (or client-side). A transition to server-side means that the game would need to be hosted on a server and players directly interact with the server instead of through their own computers. This would come with the huge benefit of a significant decrease of possible cheating methods without needing to dive into the big problem of improving anti-cheat systems (Lehtonen, 2020, p.67).

This is a tradeoff problem, where to allow an anti-cheat program to detect more cheat programs, it would need to be more invasive (John & Guigo, 2014, p.6). The best anti-cheat systems are at the kernel-level; however, the similarity of this high access system and a kernel-level malware, like a rootkit (Suganya Gandhi, 2013, p.1), is dangerously scary and requires a lot of security precautions. Cheat programs can remain undetected as long as they run before the anti-cheat systems run (John & Guigo, 2014, p.6). They can also act through a virtual machine, where the anti-cheat is in an isolated environment, unable to interact with the main computer, let alone detect the cheat programs. Virtual machine cheating as well as many other

more invasive methods of cheating are extremely difficult problems that can be resolved by transitioning to server-sided gaming systems (Lehtonen, 2020, p.68).

Microsoft is currently researching a cloud gaming system, a server-sided system, called Outatime. I want to continue researching into their solutions of decreasing latency and whether or not it is feasible to transition to a cloud gaming environment, especially current gaming communities' opinions of this new environment (Lee, Chu, Cuervo, & Kopf, 2014, p.1). The plan is for Outatime to mimic a low-latency network, similar to that of a client-sided gaming system, through various technical methods. The main difficulty will be to develop an understanding of this experimental technology in order to develop a good transition plan from the current client-sided system to server-sided cloud gaming.

**Understanding the Temptations and Incentives of Online Cheating**

The dynamics between cheat and anti-cheat developers are very interesting, almost similar to that of a chess game. It is an arms race between the developers of one software investing resources and developing new technology in order to beat the other. Of course, the incentives for this arms race are rather obvious, financial gains. 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). As mentioned before, anti-cheat developers are always at a disadvantage since users always have the capability to ensure that a cheat program will run first.

Instead of finding a technical solution and continuing the arms race, a deeper understanding of the reasonings of why people cheat and even what people consider as cheating will allow for further exploration into other technical or non-technical solutions (Chen & Ong, 2018, p.276). With the main incentives of many cheat developers being money from cheating players, by reducing the number of cheaters through appealing to their incentives with other means, the benefits of developing cheats would also be reduced. Of course, according to Russo's (2020) interview with a cheat developer, there are other developers with different reasons; however, these rather small percentage of cheat developers are not mass distributing and hurting the game as well as the profits of the company. Hypothetically, if the proposed technical solution of transitioning to a server-sided gaming system works, even though no cheat programs should be able to be installed on the server, the cheat developers would continue trying to find a way to exploit the game considering their incentives are still there, if not even higher than before. This would simply lead to a reset, but still a continuation of the arms race between anti-cheat and cheat developers.

The main challenge would be to fully and accurately represent all of the actors in this complicated arms race between developers. The TOC model can be applied: the technical actors would involve the current client-sided gaming system and the cloud gaming systems; the organizational actors would involve the anti-cheat developers and the playerbase, as well as the cheat developers and their customers; and the cultural actors could range from the incentives of all of the organizational actors to develop or use an anti-cheat or cheat software to the public perception of the transition away from the current model of client-sided games with invasive anti-cheats to a secure but potentially lesser quality performance of server-sided games (cloud games). There is a lot of research that can be used to further explore cheating in many different

forms that could provide insights in this progress, not limited to just the field of video games. Even something as simple as the definition of cheating can be rather subjective, as presented by Chen and Ong (2018, p.281), where players rationalize whether a behavior is cheating through five different mental schema.

**Intended Outcomes of the Project**

For my technical topic, I want to further understand the advantages and disadvantages of cloud gaming. Additionally, I can take in account the current and future planned technology being implemented to see if server-sided games can compete with the performance and latency of client-sided games, potentially predicting the gaming community's perception of cloud gaming. The goal is to plan out a possible and feasible transition towards a server-sided cloud gaming system. For my STS research, by understanding the motivations of cheating, I want to plot out as many relevant actors as possible onto a TOC model. Then, using actor-network theory, I can explore and determine if there are any neglected actors that can potentially lead to a different solution to satisfy the incentives of cheating instead of shutting them down with anti-cheat. With both my technical and STS, I can then make comparisons between new potential future steps of the anti-cheat and gaming industry and see which pathway would be better in the long run. I can provide meaningful recommendations for the industry on how to decrease cheating presence without treading on the invasion of players' computers and data security.

Word Count: 1669

**References:**


- 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

- Suganya Gandhi, D. & Suresh Kumar, S. (2013). Detecting the Rootkit through Dynamic Analysis. *International Journal of Science and Research*. Retrieved from https://www.ijsr.net/

- John, Joel & Guigo, Nicolas (2014, Mar 26-27). *Next Level Cheating and Leveling Up Mitigations* [Conference presentation abstract]. Black Hat Asia 2015 Convention, Marina Bay Sands, Singapore.

- K. Lee, D. Chu, E. Cuervo, & J. Kopf (August 2014). Outatime: Using Speculation to Enable Low-Latency Continuous Interaction for Cloud Gaming. *Microsoft Research*. Retrieved from https://www.microsoft.com/en-us/research

- 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.

- Mamerow, Michael (2021). Why Do Cheaters Cheat in Video Games?. *Raise Your Skillz*. https://raiseyourskillz.com

- McFerran, Damien (2016, February 8). Code Red: The history of the cheat. *Redbull*. https://www.redbull.com/int-en/

- L. Radvilavicius, L. Marozas, & A. Cenys (2012). Overview of Real-Time Antivirus Scanning Engines. *Journal of Engineering Science and Technology Review*, 5(1). Retrieved from http://www.jestr.org

- 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