Dún Laoghaire Institute of Art, Design and Technology (IADT)

Investigation into the ethical concerns of anti-cheat software

Creative Computing (DL836) - Year 4
Professional Development & Critical Thinking

Jonathan Berkeley (N00181859)
5-4-2022

Table of Contents

1 Introduction

This report will investigate and outline the potential ethical concerns and questions surrounding the development and distribution of anti-cheat software.

Anti-cheat software is developed to counteract cheating behaviour in online multiplayer games. Cheating in multiplayer games is typically accomplished through the development of software that modifies the player's game to give an unfair advantage.

This behaviour has become a serious problem in many online games, and the development of anti-cheat software to reduce cheating has become a large market in recent years (Owler, 2022a; Owler, 2022b; Dnb, 2022). As time goes on, cheating software becomes more and more complex, and the anti-cheat software has to evolve to this and become complex as well. This effect has been frequently described as a "cat and mouse game" (vmcall, 2020; Warren, 2021).

2 Context and terminology

This section will briefly outline the terminology and concepts needed to understand the rest of this report. To keep up with the evolution of cheating software, effective and popular anti-cheat software has become more invasive. Anti-cheats containing a kernel level module has become the new standard (mirageofpenguins, 2020). The kernel is the level of an operating system that has the most control, sometimes also called Ring 0. Code running at this level has the privilege to do almost anything that it wants to, with far more permissions than regular applications.

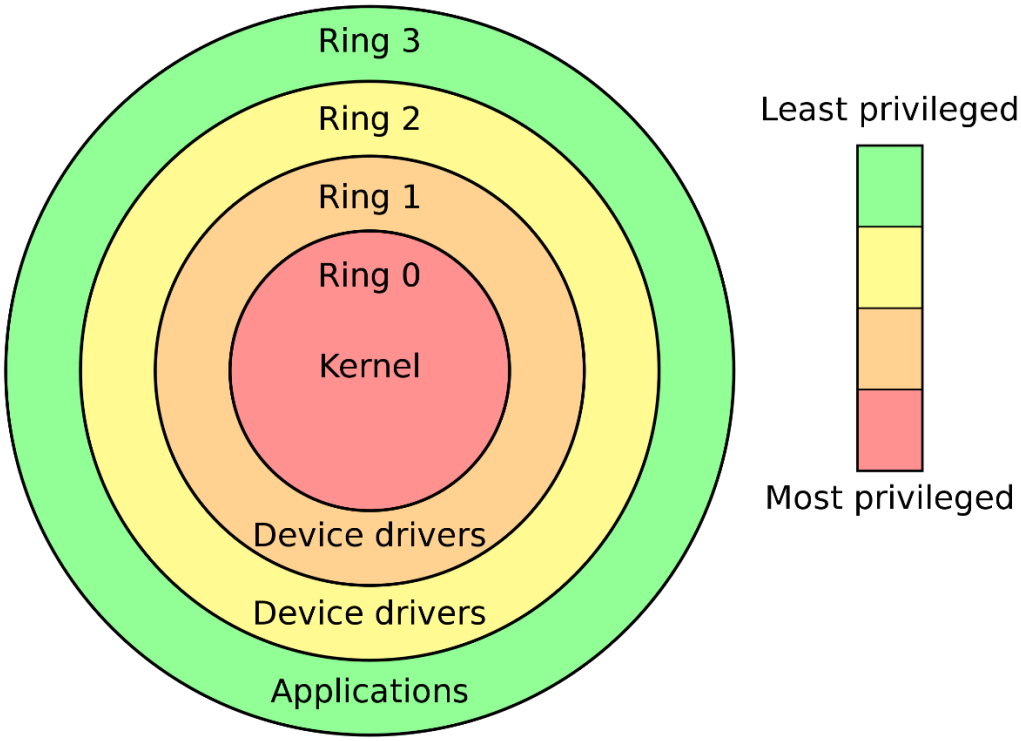

Figure 1 – Privilege rings for x86 in protected mode (Wikimedia, 2019).

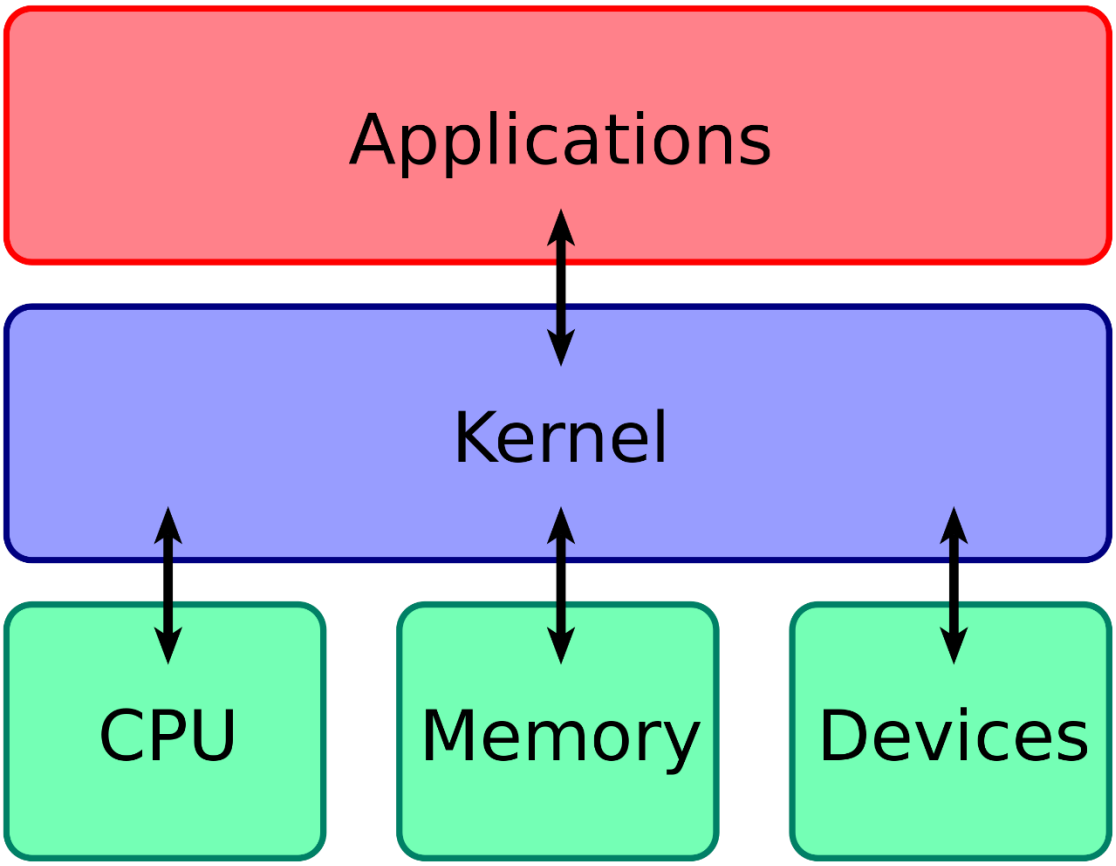

Figure 2 - High level overview of the role of the kernel (Wikimedia, 2016)

Figure 1 illustrates the concept of protection rings, however, in real systems such as Windows there are usually only two or three rings of protection depending on the version. Code in Ring 3 has the least privileges, in Windows this would be application code with no admin rights. Anti-cheat solutions created in the early 2000s consisted of code in Ring 3, but in recent years there has been a major shift to Ring 0 anti-cheat to counter cheats which have also moved to Ring 0.

Figure 2 demonstrates the role of the kernel, it provides an interface between the hardware and applications. It also contains a large portion of operating system logic. Importantly though, it controls information that applications have access to, and can also read information from applications. Essentially anything that the operating system can do, code that is running at this level can do.

As a simplification, the only thing that can prevent code executing in the kernel from doing what it wants is other code executing in the kernel. This raises the issue that when cheaters move their code to the kernel, anti-cheat solutions are forced to do the same in order to effectively detect their presence and prevent them.

3 Ethical considerations with kernel level anti-cheat

Anti-cheat software that operates at this level works by taking in identifying information about the computer, scanning all applications and having access to any data that it wants. Anti-cheat software will routinely send data samples back to its' authoritative server for manual review, this data can potentially contain sensitive information (Lehtonen, 2020).

3.1 Informed consent

Consenting to such a service isn't very explicit. Anti-cheat is bundled with videogames, and whilst the user is made to accept the terms of service which outline the software's behaviour, the majority of people that run this software do it without understanding the implications of it. Videogames are often targeted to younger audiences, which raises a serious ethical question if underaged people can consent to this level of monitoring by independent companies.

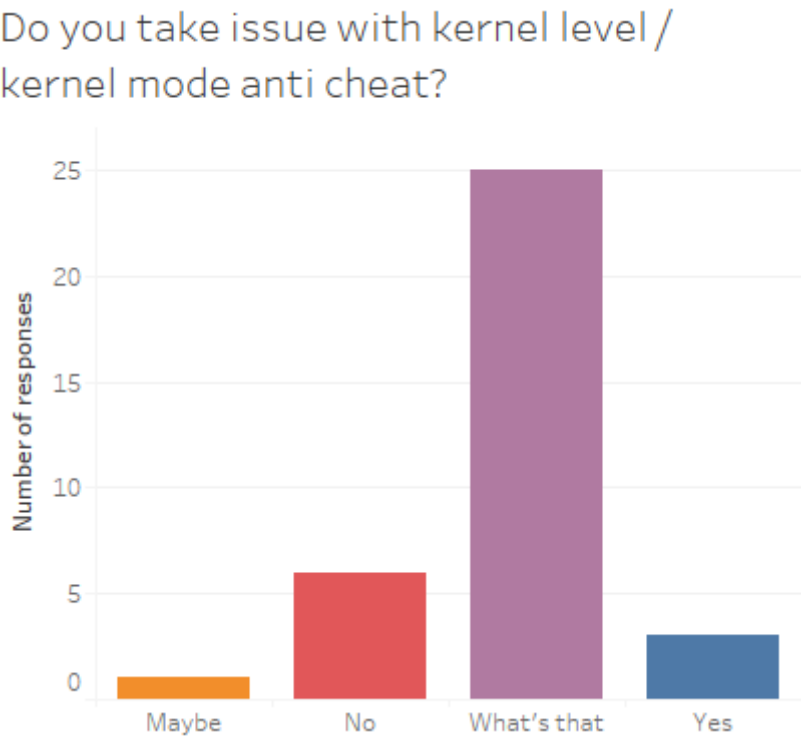

Figure 3 - Bar chart showing results for survey question "Do you take issue with kernel level / kernel mode anti cheat?"

In a survey with 35 respondents that was given to gamers, the question "Do you take issue with kernel level / kernel mode anti cheat" was met with the response shown in Figure 3. The majority of respondents did not know what that meant, despite the likelihood of them having accepted the terms of such an anti-cheat, considering the huge number of games that now employ a kernel level anti-cheat (Deni Latić, 2022). Of those that did know about kernel anti-cheat, there was a divided opinion on whether they took issue with it.

BattlEye is one of the industry leading anti-cheats. From BattlEye's End User Licence Agreements, the following terms are included verbatim.

1. "BattlEye may scan Licensee's entire random-access memory (RAM), and any game-related and system-related files and folders on Licensee's system using cheat-program-identifying algorithms, report results of such algorithms to other connected computers and/or to Licensor and store such information for the sole purpose of preventing and detecting the use of cheat programs. BattlEye only scans and/or reports data which absolutely needs to be scanned and/or reported to meet this purpose."

2. "BattlEye may further report and store Licensee's Internet Protocol address, game account name and identifier, in-game nickname, and system-related and hardware-related information including, but not limited to, device identifiers and hardware serial numbers."

3. "Licensee acknowledges that the invasive nature of BattlEye is necessary to meet its purpose and goal of preventing and detecting cheat programs."

BattlEye is used as an example in this case, however, other leading anti-cheats have similar terms (BattlEye, 2022).

While anti-cheat companies usually promise they do not collect user-identifiable information such as name and addresses, this point is typically irrelevant in practice as the anti-cheat is linked up with the game account of the player which will contain underlying personally identifiable information. The anti-cheat is required to be linked to game account information in some way in order to be able to enforce bans when cheating is detected.

Compacting the problem, some popular kernel level anti-cheats such as Xigncode3 have allegedly contained very invasive functionality that was not mentioned in the terms of use (Greidanus, 2017).

In a survey of 2,000 US consumers by Deloitte, they found that 91% of respondents accept terms and conditions without reading them, and of respondents between the ages of 18 – 34, that rate was 97% (Deloitte, 2017). The latter figure is especially important as that makes up the age demographic that video-games are targeted towards.

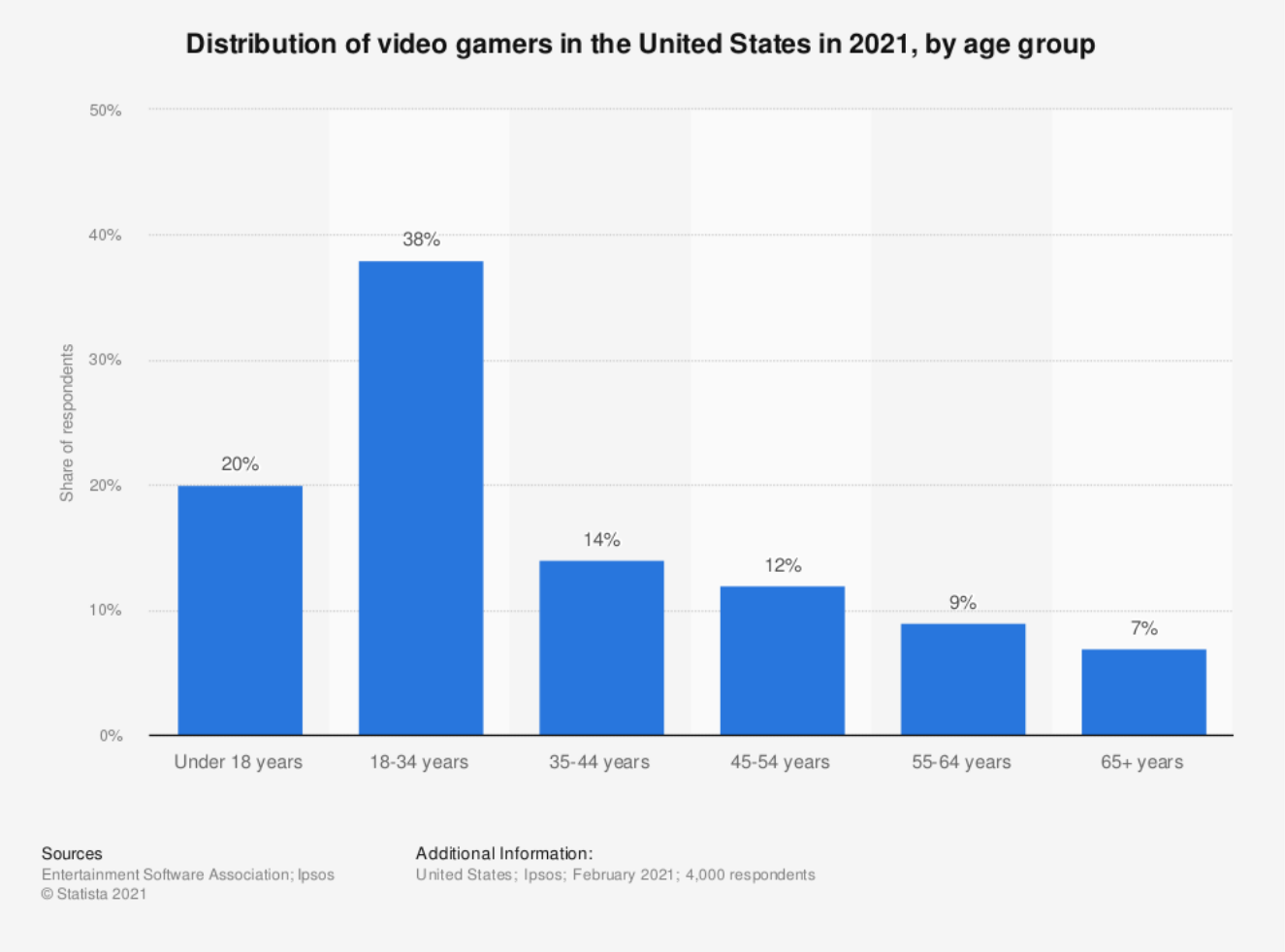

Figure 4 - Bar chart showing distribution of video gamers in the United States in 2021, by age group (Statista, 2021)

Figure 4 shows the distribution of the age of video gamers in the United States in 2021. The largest group is the same distribution that the Deloitte study found to be least likely to read terms and conditions (Deloitte, 2017). It's clear from these two studies that the vast majority of people with anti-cheat on their computers are unaware of its capabilities.

Another critical factor to consider is that the functionality of these anti-cheats is updated over the network frequently. This means that additional features can be added without the user knowing, and as anti-cheat software is highly secretive, the average user will never know when or what features are being sent to their computer.

3.2 Controversies

In 2013 an invasive anti-cheat created by ESEA was found to have been secretly mining bitcoin on player's computers, abusing the trust that the clients had put into the software. A rogue employee updated the anti-cheat for their own benefit (Savage, 2013). Mining cryptocurrency with GPUs reduces their lifetime significantly over time, and modern GPUs are expensive components to replace (Whitwam, 2021). For this breach, ESEA was fined $1 million (McMillan, 2013).

The anti-cheat software "Vanguard", has been one of the most controversial in recent years, due to being one of the most sophisticated and intrusive anti-cheats to date. This anti-cheat starts when the computer starts, and runs all the time. This means that even when the player is not playing the game, the anti-cheat is active on their computer (Mallick, 2020).

3.3 The counter-argument

Counter arguments by anti-cheat companies and security researchers alike make points that need to be considered to understand this ethical problem fully.

In a security researchers' article, the author points out that while anti-cheat is potentially privacy invasive, this invasiveness doesn't come from the fact that the anti-cheat has a kernel module. Software without any kernel functionality can be malicious and invade privacy, so it's not unique to software incorporating kernel level drivers (vmcall, 2020).

Additionally, there would be essentially no way for a user-mode anti-cheat to detect cheats that use kernel drivers. If an anti-cheat wants to protect games from modern cheating threats, they have no choice but to have a kernel component (vmcall, 2020).

4 Conclusion and recommendations

The most pertinent ethical question that this report has identified is whether or not the consumers of the anti-cheat software are aware of what they are consenting to.

Cookies that run on websites now have to explicitly list their functionality and purposes in the European Union (European Union, 2019). Cookies have far fewer potential capabilities than anti-cheat software yet consent for anti-cheat functionality is typically bundled with other license agreements that the youthful intended userbase is very unlikely to read or comprehend as this report has established.

However, this software has become a necessary evil to allow competitive integrity in online multiplayer games. Due to this, this report recommends that the most ethical approach is to be open and forthcoming about data that is collected on the client's computer and why, similar to the system that is in place for tracking and cookies in the European Union through GDPR. Videogames should also be open about the anti-cheat solutions that are in place, and be transparent with potential privacy and security risks.

Certain existing anti-cheats have taken to the approach of transparency already, such as Vanguard which runs a blog describing the features enabled and the privacy measures in place (Riotgames, 2020).

A high level of transparency should become the standard for anti-cheat software providers, with consent to invasive features being explicit asked for, and not buried in an end user licence agreement or terms of service.

5 References

BattlEye. (2022). *BattlEye EULA*. Battleye.com. https://www.battleye.com/downloads/EULA.txt

Deloitte. (2017). *Global mobile consumer survey: US edition*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf

Deni Latić. (2022, March 3). *Every game with kernel–level anti–cheat software*. LEVVVEL; LEVVVEL. https://levvvel.com/games-with-kernel-level-anti-cheat-software/

Dnb. (2022). *EasyAntiCheat*. Dnb.com. https://www.dnb.com/business-directory/company-profiles.easyanticheat_oy.250be03e7be2b8476739b62092dbe167.html

European Union. (2019, May 9). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.eu. https://gdpr.eu/cookies/

Greidanus, R. (2017). Client-side anti-cheat in online games: Legal implications from a privacy and data protection perspective. In *Arno.uvt.nl* (p. 38). http://arno.uvt.nl/show.cgi?fid=142935

Lehtonen, S. (2020). *Comparative Study of Anti-cheat Methods in Video Games*. https://helda.helsinki.fi/bitstream/handle/10138/313587/Anti_cheat_for_video_games_final_07_03_2020.pdf?sequence=2&isAllowed=y

Mallick, A. (2020, May 28). *Valorant Vanguard: The story behind the world's most sophisticated anti-cheat system*. Sportskeeda.com; Sportskeeda.

https://www.sportskeeda.com/esports/valorant-vanguard-the-story-behind-world-s-sophisticated-anti-cheat-system

McMillan, R. (2013, November 19). *Gaming Company Fined $1M for Turning Customers Into Secret Bitcoin Army*. Wired; WIRED. https://www.wired.com/2013/11/e-sports/

mirageofpenguins. (2020, February 3). *Anti-cheat kernel driver - League of Legends*. Leagueoflegends.com. https://www.leagueoflegends.com/en-pl/news/dev/dev-null-anti-cheat-kernel-driver/

Owler. (2022a). *BattlEye top competitors or alternatives*. Owler; Owler Inc. https://www.owler.com/company/battleye

Owler. (2022b). *Easy top competitors or alternatives*. Owler; Owler Inc. https://www.owler.com/company/easy17

Riotgames. (2020). *A message about Vanguard from our security & privacy teams*. Riot Games; Riot Games. https://www.riotgames.com/en/news/a-message-about-vanguard-from-our-security-privacy-teams

Savage, P. (2013, May). *ESEA release malware into public client, forcing users to farm Bitcoins [Updated]*. Pcgamer; PC Gamer. https://www.pcgamer.com/esea-accidentally-release-malware-into-public-client-causing-users-to-farm-bitcoins/

Statista. (2021). *U.S. average age of video gamers 2021 | Statista*. Statista; Statista. https://www.statista.com/statistics/189582/age-of-us-video-game-players/

vmcall. (2020, April 17). *Why anti-cheat software utilize kernel drivers*. Secret Club. https://secret.club/2020/04/17/kernel-anticheats.html

Warren, T. (2021, October 13). *Call of Duty's new anti-cheat system includes a kernel-level driver to catch PC cheaters*. The Verge; The Verge.

https://www.theverge.com/2021/10/13/22724037/call-of-duty-ricochet-anti-cheat-system-kernel-level-driver

Whitwam, R. (2021, July 30). *Buyer Beware: Crypto Mining GPUs Lose 10 Percent Performance Every Year - ExtremeTech*. ExtremeTech. https://www.extremetech.com/gaming/325337-crypto-mining-gpus-lose-10-performance-every-year

Wikimedia. (2016). *Kernel layout*. Wikimedia.org. https://commons.wikimedia.org/wiki/File:Kernel_Layout.svg

Wikimedia. (2019). *Privilege rings*. Wikimedia.org. https://commons.wikimedia.org/wiki/File:Priv_rings.svg

Young, R. (2020, April 12). *Riot Accused of Invasive Always-Running Valorant Anti-Cheat*. Game Rant; GameRant. https://gamerant.com/valorant-anti-cheat-intrusive-always-on/