The Monitoring Process In Video Games

Ruwaid Louis, ruwaid@kth.se
Henrik Mellin, hmellin@kth.se

March 2020

Contents

1 Introduction

Today, the gaming industry is a massive industry with total revenues reaching over 100 billion dollar during 2018 [11]. The competition is fierce with companies trying to make their games as appealing as possible to attract more customers. However, getting the customer to buy the game is not enough, the games needs to run smoothly for its users to keep playing the game. This is where video game monitoring comes into play.

2 Background

2.1 Video Games

Video games are becoming increasingly more popular hobby. A lot has happened since the early days of video games. A wide variety of video game genres have been introduced, for example first-person-shooters, role playing games and strategy games. Different platforms on which you can play games have also been created, ranging from hand-held, mobile, console and even virtual reality [21]. Some people even take video games so seriously that they play them competitively and compete in tournaments. The amount of money involved in so called "e-sports" is huge, for example did Dota 2 tournament "The International" have a prize pool of over 30 million dollars in 2019 [14].

2.2 Devops & Monitoring

DevOps or "development operations" is the practice of streamlining the development process in order to deliver products faster to the customers. There are several steps in the so called "DevOps cycle", such as building, testing and deploying. The last step in the cycle is "monitoring" in which the developers monitors how their product is being used. There could be several reasons to monitor your users activity. You could for example find bugs, see if the product is being used in the intended way and look for ways to improve your product [17]. Monitoring is being used in many different areas and video games are no exception. Video game developers monitor their users activity using a wide variety of metrics which will be discussed later. Then they use these metrics to for example find bugs, mitigate attacks on their servers and prevent cheaters in their games [11].

3 Monitoring

In this section we will go through the process of monitoring in video games, specifically what methods and tools are used as well as what data is analysed, for different purposes.

3.1 Anti-Cheat

Since the beginning of online gaming has cheaters been a problem. Cheaters in video games finds some way that gives them an unfair advantage compared to other players who play the game normally. One common way of cheating is using third-party applications that assist them in some way. One classic example, which is well known within first-person-shooters is "aim-botting". This is when a player uses an application which scans the screen for targets and instantly moves the the cross-hair to their heads when it has found one [1].
Cheating affects both the players of a game and the company who develop them. Players get frustrated when they face off against cheaters because it is often impossible to win against players with such advantages. And if a game has a reputation of having a problem with cheaters then fewer people will buy the game, which affects the company who develop them. Due to this, there has been extensive efforts in preventing cheaters throughout the years. However, even with better anti-cheat systems, the cheaters find new ways to work around them and because of this cheating is still a problem in today's online games [6].

Methods

There are countless tools that provide anti-cheating services. Perhaps the most well known service is VAC, or Valve Anti-Cheat. VAC's primary function is to scan the systems of their users in search for cheating software. If such a software has been detected VAC will permanently ban the player from playing on their servers. There are other tools such as "PunkBuster" and "NProtect GameGuard" that operates in a similar fashion [9]. There has been talk about the integrity aspect of prying on users personal computers in order to find cheating software. Since you are forced to use these anti-cheating software when playing online-games some people believe that it's an attack on their privacy to have their computer searched. However, today has software like this become the standard in most online-games despite its integrity issues [7].
Another method which is widely used is crowd-sourcing the anti-cheat detection to its players. If a player feels it is playing against someone with cheats that he or she is given the option to report that player for cheating. After a player has been reported that player might be scrutinized either by the games anti-cheating system or by other players who gets to review the actions of the alleged cheater. After enough data has been gathered, a verdict can be reached on whether the player was cheating or not [19].

Data

Since the developers of anti-cheating software do not want their software to be worked around or reverse engineered, they do not want to disclose details on how their software works or what kind of data it collects [15]. But as previously mentioned anti-cheating software collects data about what programs a user is running while the user plays their game.
Another common way of cheating is botting. Botting is when you use software that controls your character and makes it perform certain actions automatically. The anti-cheating software collect data about the actions of their players and see if it matches the behaviour of known bot programs. If a match has been found the player might face punishment in forms of banishment [10].

3.2 Attacks

Online based games such as online multiplayer games or browser based games which require server are one of the most popular games found on the market today.[18] A direct effect of being available on the internet is being vulnerable to remote and malicious attack and online video games are no exception.[3][22] It is therefore very important to monitor for such attacks so that one can detect them and stop them as soon as possible as not to disrupt the service to the players or leak sensitive information. This contributes directly to the confidentiality, integrity and availability of the service.

Methods

DNS - Dynamic Name System is a big threat to security because of its high vulnerability. Therefore it requires monitoring to prevent attacks.[11] DNS monitoring is a tool often used to look for DNS hijacking, provider issues or DDoS - Distrubuted Denial of Service attacks. Sometimes a mapping tool is used which shows a visual representation of the information on clients connected to the server amongst other things which can help to identify a malicious intent.[2] Monitoring network activity is a must, but there are many ways to go about doing this and there is no industry standard. Some companies choose to outsource this kind of work to more specialised companies.[16] But for any intents and purposes there are plenty of tools out there to help one with securing their network.[4]

Data

Network activity data can be analysed to detect attacks such as a DDoS attack or other disruptive attacks by looking at the amount of connections made and comparing to normal usage to find out if there are any disturbances which could link to a malicious intent. However since IP Spoofing is a common disguise technique, one can do a Web Test to validate the IP address of the website accessing the service. Diving deeper into network errors, one can monitor the HTTP data being sent and received as well as any SSL - Secure Socket Layers

connections, specifically for any errors. This is a more tedious task since there may be thousands of HTTP responses being sent per minute making this type of monitoring inefficient but adds more security which is common trade-off in any security practice. Moreover if the service is hosted on a website then monitoring user flow data can be useful to find a pattern in the user journey which could indicate an error or an attack.

3.3 Bugs

Too often, after a video game has been released, new bugs are is found in the game which can sometimes make the game unplayable.[5] This hurts both the developers and the companies reputation which means it needs to be avoided. But it is hard to always find all bugs riddled in the game before a release date. Therefore one can monitor games after release to look for eventual bugs and be quick with releasing patches before said bug affect too many players.

Methods

Runtime monitoring or also called Runtime Verification is a tool which can be used to monitor for bugs in video games and involves the process of looking for any data which show deviation from intended software behaviour.[20] The game code can be instrumented to alert whenever the software reaches a state which does not comply to the wanted software behaviour. Another tool is seeing a game as Temporal Logic Constraints and alert whenever a predicate is not true which should always be true.[13]

Data

What type of data which should be monitored is very game specific. But generally one type of data which is often used to monitor for any bugs is player position. Players are very often confined to a given space, so whenever a player goes out of these boundaries it should be a clear sign of a bug within the game. Other useful data such as player velocity, gold amount or stats can also show signs of existing bugs by being vales over or under the constraints. For example, in some games, there is no such thing as a negative amount of gold. It is therefore alerting if there would so happen to be a player with a negative amount of gold. An example of this is in testing Super Mario World where Mario's jump height should never exceed five units.[20]. Any data which has any kind of constraint can be used in monitoring for bugs by simply adding an alert whenever a constraint has been violated.

3.4 Performance

As a constant reminder of how important it is to have a well performing game, we have the FPS - Frames Per Second counter which determines how well your system handles the graphical performance of the video game.[12] Too reach a wider audience as well as being more enjoyable to play, improving a game's performance is an essential part of game development. Much of the performance optimization of a game is done prior to release but once released it may be played on systems which haven't been tested and optimized for as well as new components being released. Different architecture may require different optimizations. It is therefore important to monitor for performance issues which may occur and use the data to find out how to optimize the game further.

Methods

How well a game performs on a system can depend on many factors and some factors are non-existent for some games. For massive multiplayer online games which aren't graphically demanding, network performance can be the biggest factor in ensuring a lag-less game experience. While for offline games that factor is non-existent, instead in these games, how well the game runs on the system may be more important. Therefore to monitor performance some may refer to monitoring the network while some use the FPS counter as a metric of performance and try to increase it's value with code optimization etc. However, monitoring offline games remotely will probably still require an online connection to send needed data to the company to analyze. In general Resource Monitoring can be an efficient method to analyze the performance of a video game in a system, especially in mobile games where it is of great importance to have a well performing game.[8]

Data

When monitoring network activity for performance purposes it is often so that almost the same things are monitored as mentioned in 3.2.2. This is because of the similar task, ensuring a stable network with good flow. When profiling the performance of a game within a system, one can look to data such as:

- CPU - Central Processing Unit usage
- GPU - Graphics Processing Unit usage
- Memory usage
- FPS counter

Although the FPS counter shows how good a system handles the game, it is not a good measure of the optimization of the game code since computers will vary a lot in performance. As well, a high FPS counter does not mean the game runs seamlessly, that's why looking into the usage percentage of the GPU and CPU is important because it shows whether or not the game is hoarding the computers

resources. Although the data may show indication of a bad performing game, it will most probably not show where the issues are. That is up to the developer to find out and fix.

4 Conclusion

There's a lot of data to monitor if one intends to cover all fields. But the type of data which is of most importance will depend on the type of video game. Companies can therefore choose to focus more on what is most important for their game. For some purposes there are more established methods to be used while for others, there are only some considerably inefficient methods at disposal. However, for all intents and purposes there's a method and tools to be used which can help. It is of great importance to make sure that a released game is monitored and issues patched as not to cause negative responses from the community which may affect the company. Working pro-actively in the gaming industry is essential to keep customers pleased given how many different issues which can occur and may go unnoticed without any monitoring activity.

References

[1] Tarantola Andrew. A brief history of cheating at video games, June 2019.

[2] Muhammet Baykara, Ugur Gurturk, and Resul Das. An overview of monitoring tools for real-time cyber-attacks, 03 2018.

[3] Matthew Cook. Why online video gaming will be the next industry under cyber attack, May 2016.

[4] Bojana Dobran. 35 network security tools you should be using, according to the experts, Mar 2020.

[5] Ben Gilbert. Why are so many video games broken at launch?, Nov 2014.

[6] Nelson Granados. Report: Cheating is becoming a big problem in online gaming, April 2018.

[7] RUBEN GREIDANUS. Client-side anti-cheat in online games: Legal implications from a privacy and data protection perspective.

[8] Ville-Veikko Helppi. Performance profiling and monitoring for mobile games under development, Aug 2019.

[9] Reginald Jimenez. Top 05 anti-cheat software to make fair for gamers., May 2018.

[10] Ah Reum Kang, Seong Hoon Jeong, Aziz Mohaisen, and Huy Kang Kim. Multimodal game bot detection using user behavioral characteristics. *SpringerPlus*, 5(1):523, 2016.

[11] Kameerath Abdul Kareem and Kameerath Abdul Kareem. Monitoring in the gaming industry - dzone performance, Jun 2018.

[12] Michael Klappenbach. How to optimize and improve graphics performance and frame rates, Feb 2020.

[13] Axel Legay and Saddek Bensalem. *Runtime Verification: 4th International Conference, RV 2013, Rennes, France, September 24-27, 2013, Proceedings*, volume 8174. Springer, 2013.

[14] Liquipedia. The international 2019, Aug 2019.

[15] Gabe Newell. Valve, vac, and trust, 2014.

[16] Brent R Rowe et al. Will outsourcing it security lead to a higher social level of security? *Repository Home*, May 2008.

[17] smartbear. What is devops monitoring?

[18] Statista. Online games - worldwide: Statista market forecast.

[19] Valve. Overwatch faq.

[20] Simon Varvaressos, Kim Lavoie, Sébastien Gaboury, and Sylvain Hallé. Automated bug finding in video games: A case study for runtime monitoring. *Comput. Entertain.*, 15(1), March 2017.

[21] Vince. The many different types of video games & their subgenres, April 2018.

[22] Chen Zhao. Cyber security issues in online games. *AIP Conference Proceedings*, 1955(1):040015, 2018.