Cheating in Massively Multiplayer Online Games and Associated Security Issues

Term Research Paper

Kirby Lo

7/3/2013
Cheating in Massively Multiplayer Online Games and Associated Security Issues

Introduction

In the past decades, the lifestyle that faced developed countries such as those in North America, Europe and some parts of Asia has changed drastically. Since the 1960s, leisure time has increased by an average of 6-7 hours per week for men, and 4-8 hours per week for women\(^1\). This has lead people to rethink what they do in their leisure time, and created a market for activities to fill up such time. One of the inventions that arose, combined with the development of computing technology, was video games. With roots in America as early as 1947\(^2\), video games have grown from simple pixels moving on the screen to a mainstream pastime. With the development in network technology and the World Wide Web, it was inevitable that video games, along with much of the tasks and activities of our everyday lives, would utilize this platform and join the globalized community of the Internet.

History and Overview

The video gaming industry was estimated to bring in revenues of $66 billion dollars\(^3\) in 2013, and growth has been strong in social and mobile gaming particular, and is expected to grow from 5.8 billion to 8 billion dollars globally. As the industry reached out to more and more people, gaming became more social and more commonly accepted in society; combined with increased affordability, what was once considered a hobby for kids and outcasts became mainstream, and many children grew up while maintaining the same habits. As a part of this rapid expansion, Massively Multiplayer Online games (MMOGs) were developed to cater to the increasingly interconnected world. MMOGs are typically based on a fantasy setting, where each player creates a personalized avatar and adventures in the virtual world. In one such MMO, EVE online (EVE), where a user is placed in a futuristic setting as a spaceship pilot, 65303 users were recorded to be online concurrently in a single, though distributed, server\(^4\). This would place them 205\(^{th}\) in the world by population, had EVE been a country and its users considered to be residents of that country. Many of the MMOGs run on a subscription basis, where the user pays a monthly fee to access the game, and some other games are free-to-play (F2P), but contain micro-transactions where the users can pay money to augment their characters or accounts. World of WarCraft (WoW), one of the most successful MMOGs of all times, places the users in the fictional world of Azeroth and challenges the users to adventure to strengthen both the user’s character and fictional armory through epic quests and dungeons. At its peak, WoW garnered 12 million subscribers, with each user paying approximately $15 per month to access the game, demonstrating that video game is clearly no longer child’s play, but rather, a significant market where a great deal of money is changing hands.

---

\(^1\) Aguiar  
\(^2\) Goldsmith  
\(^3\) Nayak  
\(^4\) EVE Online
It is not only the developers that are profiting from the rise of MMOGs; virtual weapons, virtual characters, virtual real estate, and even virtual hairstyle have created a secondary market in which users buys and sells virtual goods that are attained within the game for real currency. In 2008, Cikicm and Lehmann, in their paper “Cheat-Prevention and Analysis in Online Virtual Worlds,” discuss the increasing importance of placing real value of virtual property. The real money trade of virtual items has an estimated volume of $2 billion per year as of 2007, and it has risen considerably since then. As games become more mainstream and more complex at the same time, it becomes increasingly difficult to track the exact value or volume as game companies are typically reluctant to release such valuable business information to the public.

With so much money on the line, it is clear that it is in both the development companies and the users’ best interest to keep the game running smoothly. Companies have a vested interest in keeping their users happy so they continue subscribing or purchasing from them, and MMOGs have shown to be pioneers in cloud computing. While this range from game to game, some of the more sophisticated games such as EVE and WoW use server clusters that perform calculations to return to the user as well as render much of the game world in real time. Even for companies that are not directly involved in the gaming business, MMOGs are a way to observe the associated strengths and weaknesses of operating a platform on a cloud. As an example of how seriously many companies now take cheating in MMOGs, EVE online actually has a whistleblowing petition system with which users can report other users that is hacking, disrupting the virtual world, abusing bugs, or

---

*Figure 1 - Video Game Market Data 2012/Estimated 2013*
Cheating in Massively Multiplayer Online Games and Associated Security Issues

Cheating in MMOGs

While there are no universal views on what constitutes cheating, as it is typically very context-specific and subjective, there are very often instances of perceived cheating or injustice within the context of the MMOG world. Yan and Randell\(^9\) provides a taxonomy of common forms of cheating in online games, divided into cheating that is of special relevance to online games and generic forms of cheating as shown below in Table 1.

<table>
<thead>
<tr>
<th>Type</th>
<th>Label</th>
<th>Cheating Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of special relevance to online games</td>
<td>A</td>
<td>Exploiting Misplaced Trust</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>Collusion</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>Abusing the Game Procedure</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>Cheating related to Virtual Assets</td>
</tr>
<tr>
<td></td>
<td>E</td>
<td>Exploiting Machine Intelligence</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>Modifying Client Infrastructure</td>
</tr>
<tr>
<td>Generic</td>
<td>G</td>
<td>Timing Cheating</td>
</tr>
<tr>
<td>Of special relevance to online games</td>
<td>H</td>
<td>Denying Services to Peer Players</td>
</tr>
<tr>
<td>Generic</td>
<td>I</td>
<td>Compromising Passwords</td>
</tr>
<tr>
<td></td>
<td>J</td>
<td>Exploiting Lack of Secrecy</td>
</tr>
<tr>
<td></td>
<td>K</td>
<td>Exploiting Lack of Authentication</td>
</tr>
<tr>
<td></td>
<td>L</td>
<td>Exploiting a Bug or Design Loophole</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>Compromising Game Servers</td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>Internal Misuse</td>
</tr>
<tr>
<td></td>
<td>O</td>
<td>Social Engineering</td>
</tr>
</tbody>
</table>

Within this framework, Yan and Randell identified the vulnerabilities within the underlying form of cheating, the consequences and the cheating principal. This focus of this paper is on reviewing the potential security issues that is associated with cheating within online games, so additional emphasis will be placed on consequences that creates potential security issues for the company. Yan and Randell focuses on the four traditional aspects of computer security: confidentiality, integrity, availability and authenticity. An additional category of fairness violation was also included to address the specific context of MMOGs, but this paper will not address this category as it is largely irrelevant when discussing potential security violations.

---

\(^7\) EVE Online Dev Blogs
\(^8\) Woo
\(^9\) Yan
Cheating in Massively Multiplayer Online Games and Associated Security Issues

Table 2 - Classification of Online Game Cheat by Violation

<table>
<thead>
<tr>
<th>Violations</th>
<th>Violators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>G</td>
</tr>
<tr>
<td>Authenticity</td>
<td>K</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>A, B, I, J, O</td>
</tr>
<tr>
<td>Integrity</td>
<td>A, F, H, J, M, N</td>
</tr>
</tbody>
</table>

Faced with risks in so many areas, it is important for management and users alike to understand the risks associated with MMOGs and how to manage risk. Risk management involves understanding the vulnerability and threat and determining appropriate countermeasures to reduce the risk to an acceptable level.\textsuperscript{10} This paper will look at four of the key concepts in information security with respect to MMOGs and review examples of vulnerabilities, threats, countermeasures and impact on the MMOG administrators as well as users.

Countermeasures must not only be evaluated by its effectiveness in preventing cheating, but on other qualities as well such as preserving real-time quality and privacy issues.\textsuperscript{11} Anti-cheat implementation often causes false positives, otherwise known as type I errors. This is, to the users, a more serious issue than type II errors, which are false negative. While users would like their game to remain cheat free, it is more directly harmful to them that their right to play the MMOG is revoked because of a false positive. Many game companies have taken up a less stringent stand on cheating in order to retain business, only temporarily banning first time offenders, hoping that they will stop cheating in the system.

**Availability**

Availability refers to the availability of the gaming platform to the users. This is an area that would be of particular importance to users, as many MMO operates on a subscription basis, and when the platform or servers are down, users feels dissatisfied as they are unable to access the service they have paid for. A comparison can be drawn with the availability of cloud services and cloud apps, and for this reason, this is an area where users in other industries can learn from high profile issues as well as potential security vulnerabilities.

There are many type of cheating that would result in loss of availability to users; one such cheat or hack is known as the drop hack. Commonly found in games where there are direct matchups, such as one versus one strategy online games like StarCraft, they are also found in games such as WoW and first person shooters (FPS) increasingly. The mechanics differ; some hacks uses a similar technique to denial of service (DoS) attacks by flooding the other users, which of course would only work if the victim’s connection information is available to the hacker. Alternatively, DoS attacks against the server, which is public, is a lot easier to do, but much more difficult to succeed as corporations typically have stronger defenses against DoS attacks and additional capacity. This type of attacks is particularly difficult to prevent from a development point of view, as the best way of preventing DoS attacks is through filtering of incoming traffic as well as having additional capacity, neither of which is something that is controlled directly by the developer. Distributed DoS (DDoS) attacks are becoming more

\textsuperscript{10} ISACA
\textsuperscript{11} Pierre-Louis
frequent, and there has been a 22 percent increase in DDoS attacks in the 12 months preceding the end of the first quarter of 2013. With increased sophistication and access to DDoS attacks, it is becoming an increasingly significant issue that needs protection against to avoid downtime.

EVE Online recently was attacked by hackers employing DDoS, and it resulted in an outage of several hours, during which paying customers were unable to access their service. Skill points for use within the game were provided to compensate users. This move cost EVE’s developers nothing monetarily, but it’s important to consider the lost in goodwill, as well as the fact that compensation often would require monetary outflow in more typical industries. In compensating users with items that have monetary value, an additional problem of economy management is created: basic economics dictates that increasing the amount of currency available would devalue the said currency. It is important for developers to not simply take the easy way out and compensate users anytime an issue occur or risk disrupting the virtual economy in which many users are heavily invested in.

Availability is an important concept for users of any system as any perceived value a system provides vanishes if the system is not available. For this very reason, significant emphasis is placed upon disaster recovery plans (DRPs) and Business Continuity Plans (BCPs). With a world that is increasingly always online, the recovery point objective (RPO) and recovery time objective (RTO) becomes shorter and shorter, and implementation of redundant hardware becomes more crucial to the maintenance of availability. This creates a frustrating issue for server administrators as it is important for any server or cloud based system to be updated regularly and maintained, but it cannot update software or perform regular maintenance without taking the system down. This conundrum puts heavier emphasis than ever on the importance of a testing environment and the ability to push changes into production in a timely manner after successful user and implementation testing. However, it is difficult and costly for developers to plan for all possible contingencies; at some point, a certain level of risk must be accepted, and the loss associated with the crystallization of that said risk can be significant, and availability concerns can stem from reasons beyond malicious attacks.

WoW was originally announced in 2011 and subsequently released in 2004. That is over a decade of development and no game typically last that long. With the advent of online gaming, however, developers have the ability to have a persisting game world, but add content to it through patches and expansions. To date, WoW has had four expansions, and each of those expansions, on release, has encountered massive downtimes as players who have previously left returns to experience new content. The cyclical nature of MMOGs that have new content released over time creates a significant problem for developers: if they plan for peak load, there will be lot of wasted capacity as many users quit shortly after experiencing the new content, and subscription number falls quickly, but if they plan for the average load, then there will be significant latency issues as well as downtimes during the release of new content. In addition to the actual production servers, there would be heavy strain on the patching servers as millions of users attempt to retrieve the last patch and update their user client. Over the years, Blizzard has begun allowing pre-patching, which allows the user to download the majority of the

---

12 Prolexic
13 CPP Spielmann
14 Blizzard
patch, withholding only a small amount of data to be distributed on release date. This alleviated the strain on the patch server, but actual user load on the production servers typically remains much greater than maximum load. While Blizzard has never disclosed what it does to distribute the load, some theorizes that redundant servers that are used in case of server failure, as well as clusters from other games that Blizzard manages are used for the rush shortly after release. Even with experiences of so many patches and expansions behind them, Blizzard consistently has extended downtimes during the release day. This is an area where significant learning should be done for other companies to avoid such situations, regardless of whether it is gaming related or not.

Authentication

In IT, authenticity of data transfer and communication is important to ascertain that the data is from a trusted source and controls over authenticity often provide non-repudiation as well. In MMOGs, authenticity is important as there are often significant amount of user interaction and the lack of authenticity would result in a lack of accountability, allowing users to act irresponsibly at the cost of other users’ enjoyment. Authentication could also provide an avenue for cheaters to collect ID-password pairs through setting up a bogus game server and collect user name-password pairs.

The above describes phishing or pharming, based on the method it uses. While keyloggers have been the primary way of collecting passwords in the previous decade, phishing and pharming have had increasing success as anti-virus software become more adept at eliminating keyloggers and preventing their installation. Phishing refers to the act of acquiring confidential information by providing an input form from a trustworthy entity in electronic communication. Phishing attempts are often found on forums that users discuss various MMOG related topic and encourages the users to log in to access some sort of information. Alternatively, emailing users masquerading as the Game Master (GM) or the administrator of the MMOG they are involved with is also a strategy that is often used to some success. These emails usually include either an incentive, such as suggesting that you have won a prize, or attempts to induce panic, suggesting that your account is compromised and you must log in to change your password. These act as bait and hopes the user makes a poor decision to follow the instruction on these email owing to a temporary lapse of judgment due to greed or panic. Pharming refers to the act of redirecting a website’s traffic to another dummy site. This is done through compromising the DNS server software or by adjusting the hosts file on a victim’s computer. This is a growing approach that requires less modification to the victim’s computers and harder to detect as well, as there are nothing running the background after the initial modification is done.

Prevention mechanisms for these problems are mostly education based; it is important for the user to note which are legitimate emails and which are not. Most online services will typically never ask for your password, and such requests are typically huge red flags. Despite the logic being relatively simple, many people

---

15 Skelton
16 Xerin
17 Yan and Randell
18 Van Der Merwe
fall victim to this scam and it costs companies a significant amount to hire customer support representatives to resolve such stolen accounts, in order to retain their business. GMs of WoW recommend that user always manually type in the URL to their website in order to avoid phishing attempts, and the active promotion of the Blizzard Authenticator, which is simply a token that generate a temporary passcode that enables two-factor authentication, is Blizzard’s attempt to reduce the number of compromised accounts. Blizzard originally charged for the physical authenticator, but has since given them out in large amounts at video game conventions (such as their own BlizzCon), and they have also developed a mobile version for iOS and Android available free of charge. In addition to the initial authentication, it is also important to reauthenticate prior to any changes to user information. This is of particular importance in countries like China and Korea, where internet cafes are much more prevalent than personal computers. Users that leave their terminal unattended could easily have their passwords changed without even knowing without some form of reauthentication.

With any control procedure, it is important to balance the risk and the rewards of preventative controls. In this case, having excessive authentication in place often breaks immersion for the user and succeeds in only disrupting the user experience. One MMOG, Eden Eternal, attempts to validate the status of the user randomly to ensure that it is not an automated program playing, or botting, by having random CAPTCHA checks pop-up as you play the game. This turned out to be an extreme annoyance for players and failed to stop bots in any meaningful manner, as optical character recognition (OCR) technology available is very powerful allowing developers to automatically fill these items in, bypassing the human check. However, for users, it is time consuming and disturbs their gaming session. In recent time, there are even preset chatting functions to pretend that the botters are actual human. WoW, on the other hand, ensures that two-factor authentication is used every time you log in, but there are optional settings that allow the server to remember the computer or device you logged in from, so you will not need to reauthenticate for 2 weeks if logging on from the same terminal. Steam, a computer game distribution platform, does something similar, but uses email to send you a special one-time password each time. These are examples of controls are effective in protecting the users, without being overly obstructive and frustrating for them.

Confidentiality

Confidentiality is often the most focused upon area in information security. Confidentiality refers to protecting information assets from unauthorized access. MMOG companies often have significant amount of sensitive information, such as credit card information, customer’s personal information, as well as user name and passwords of users that may be reused on other websites and services online. This is a significant liability on the company’s point of view and any leaking of this information or unauthorized access could result in significant lawsuits. This is also an area where there is a lucrative black market for information attained, so there is additional motivation to hackers and malicious users to attempt to obtain confidential information. That, combined with the relative anonymity of the internet, creates a unique situation where many people, who would never consider committing a crime in real life, unknowingly or knowingly crosses the line for monetary gains.

---

19 Woo and Kim
As there is a lot more to gain by breaching confidentiality than any of the other security concepts, the number of attacks and cheats associated with this is also relatively higher. Within the framework detailed above, potential faults that would cause a confidentiality violation include exploiting misplaced trust, collusion, compromising passwords, lack of secrecy and social engineering. Similar to the discussion with authenticity, attacks are becoming more focused on the human aspect rather than the technological aspect, as developers provide better security in their software and games. However, without proper training to the user, security measures are much less effective, demonstrating that the user is ultimately the weakest link in the security framework.

Through some of the faults in authentication, it is possible for hackers to gain unauthorized access to information, and it is important for companies to maintain information in a way that would be functional but would still protect users. One example that has become prominent is credit card information; while you can save credit card information on websites, it would not reveal the full number to you even if you are logged in securely, because there is no need for you to see that full number. The actual owner of the card would have access to it physically, and having several digits just helps confirms which card it is for those that have multiple credit cards. Providing information on a need-to-know basis is a strong way to protect confidential information. This concept can also be applied to passwords, which are typically starred out even when you are logged in. While these controls are effective, it protects user information on an account-by-account basis, and most advanced attacks do not function in such a way.

Sophisticated cyber-attacks are often aimed at servers and database in order to get a copy of the information, which can later be sold or traded. The most effective way to protect this information from such attacks are the use of intrusion detection systems (IDS), but the discussion of IDS is out of the scope of this paper. In addition, strong encryption would render the data useless even if extracted. On April 21st, 2011, Sony’s online gaming platform PlayStation Network (PSN) and Qriocity networks were compromised and resulted in the breach of approximately 70 million user’s sensitive information, including names, addresses, dates of birth, passwords and security questions. Credit card information, while encrypted, may have also been stolen. This significant breach of confidentiality also prompted a week long shut down of the network, affecting availability as well, while Sony determine the way the attacker gained access and resolved the issue. It was until almost three weeks later that service was fully recovered and operational. Two years later, Sony Computer Entertainment Europe, the Europe branch of Sony’s gaming division, was fined £250,000, the 3rd largest fine of all time from the Information Commissioner’s Office (ICO), for the breach of the Data Protection Act in April 2011. In addition to the fine, Sony was sued shortly after the intrusion, and their share prices plummeted. This event demonstrates the severity of confidential information breaches, as well as the showing that the user cares very much in their personal information security. While the class action lawsuit was ruled in Sony’s favor, this episode

20 Richmond
21 Ibid
22 Warman
23 C, Alex
24 Google Finance
is something that operators of online platforms, whether or not it is related to gaming, can learn from. The costs to Sony were approximately $170 million, in addition to lost sales and loss of goodwill that is not as easily measurable.  

**Integrity**

Integrity is to the prevention of unauthorized modification of information and in the hands of a skilled user with a particular objective, exploitation of faults in integrity can cause significant amount of damage with respect to the previously discussed topics. Faults in integrity can be found at many levels, as information systems and MMOGs consist of many layers of applications that are all tightly integrated, and vulnerability embedded within any level could allow unauthorized changes and access to confidential information. Within MMOGs, there are those that are played online, within a browser, or those that are played through the game client that is downloaded. For those that connect to the server through a client, there a chance that client infrastructure can be modified to access data that is unintended to be available, which could lead to issues in the integrity of the system as a whole.

Cheating through modification of the client infrastructure is common within MMOGs, and one example is model editing, which changes the way the client display certain information. Opaque walls can be edited to be transparent to allow users to see through it and this would cause issues in the integrity of the game. While this is an example of a client side change that affects nothing else besides fairness and the cheater’s perspective, the ability to make changes to the client provides the ability for users to tamper the code of the client to attempt to access sensitive game state or game data that would otherwise be unavailable to the player. This could potentially allow elevated game privileges, or access to other user’s information if the ability to masquerade as a GM account is done. This again demonstrates the interconnectedness of the security principals, and how violation in one area would very often result in exposing vulnerabilities in another.

Fortunately, integrity is an area that can be secured through well-developed code and checks of the incoming information. Blizzard utilizes a software client known as Warden, integrated within WoW and other Blizzard games, to prevent cheating and protect the integrity of files. While Blizzard refuses to reveal the workings of Warden to avoid malicious users from circumventing it, there has been extensive investigation from the end user side as to how it works. Warden acts as spyware in a way, monitoring program and processes that is running in the background, and provide a hash of processes running to Blizzard. Personally identifiable information is not collected according to Blizzard, and the hash information is compared with known and detected cheat signatures to determine if there are any cheating activities going on. If Warden detects any cheat programs or alteration to the WoW client, then it will shut down the program and prevent the individual from continuing to play. The legality of this was questioned in MDY Industries, LLC v. Blizzard Entertainment, Inc., et
al,\textsuperscript{28} where the court found that WoW purchasers were not legal owners of the game software but rather licensees of the software, and violation of the End User License Agreement (EULA) was grounds for Blizzard to terminate their use of the program.

The biggest problem with anti-cheat system such as Warden and Valve Anti-Cheat (VAC) that is used for many games on the Steam platform is false positives\textsuperscript{29}, and with the internet being an open platform on which complaints can be vented, there could be significant losses in goodwill and future sales. It is important to balance having a strong stance on cheating but not hurting those who are erroneously detected and preserve the privacy of your customers. Organizations that run on clouds obviously would have fewer issues similar to this, but this demonstrates that there are very real privacy concerns and potential problems associated when operating on a cloud.

Another method employed is state exposure control, where states in the game world are released only as the user requires it. This is similar to releasing information on a need-to-know basis that was previously discussed, and would allow the developers to control what information that user has access to. For example, a user would not have the data of an enemy combatant, until that enemy is slated to move into the user’s field of vision. This type of control is typically strong and fairly effective, but has a significant downside in having increased load on the server and on the client’s CPU.\textsuperscript{30} For this reason, the less secure way of preloading data is often used as state dissemination in real time is not realistic with the existing infrastructure. With the speed of processors and internet connections rising significantly over the last decade, this is an area that should be revisited to test viability.

\textbf{Conclusion}

In this paper, Yan and Randall’s taxonomy for cheating was analyzed and used to identify potential security issues and their respective countermeasures. Through this analysis, it would appear that much of the issues and vulnerabilities found in MMOG cheating are also relevant to those experienced in distributed computing. Many of the lessons that are learned in the aforementioned security incidents should be taken to heart and further the development of anti-cheating research. As the developers continue strengthening their defenses, the attackers in-turn learn from what was ineffective and continue to grow. As it is with physical crime, intellectual crime is an ongoing cat and mouse game, and many cheat prevention and threat prevention system will soon grow out of date. With cloud computing on the rise, some of the issues identified in MMO gaming must be analyzed and taken seriously, and applied on the wider security environment.

\textsuperscript{28} MDY Industries, LLC v. Blizzard Entertainment, Inc., Et Al.

\textsuperscript{29} Valve

\textsuperscript{30} Li
Cikicm, Grottke, Lehmann-Grube

**Title:** Cheat-Prevention and Analysis in Online Virtual Worlds

**Periodical / event:** e-Forensics 2008

**Vol.** 2008

**Pages** 7

**Date accessed** May 15, 2013

**Link/location** ACM

- Cikicm and Lehmann discusses the increasing importance of placing real value on virtual property and how it is driving the trends in game security.
- Legal precedence have been set to create a market of over $2 billion dollars a year in virtual assets.
- An outline and prediction of the online world is provided discussing a lot of significant roadblocks to development such as processing power and internet bandwidth availability.
- An in-depth look on scalability and how it is limits anti cheating as it is difficult for existing processing power to analyze and review all incoming traffic without any effect on latency.

Hu, Jiakun, Zambetta, Fabio

**Title:** Security issues in massive online games

**Periodical / event:** Security and Communication Networks, 2008

**Vol.** 2008

**Pages** 10

**Date accessed** May 17, 2013

**Link/location** Wiley InterScience

- Hu and Zambetta further discuss the ramification and countermeasures to online cheating based upon the work done by Yan and Randell.
- Security countermeasures are discussed based on the security fault that the cheating activity exploits.
- Counter measures for cheating by exploiting misplaced trust, by collusion, by abusing the game procedure, cheating related to virtual assets and by timing is discussed in detail.

Li, Kang, Ding, Shanshan, McCreary, Doug, Webb, Steve

**Title:** Analysis of State Exposure Control to Prevent Cheating in Online Games

**Periodical / event:** NOSSDAV’04

**Vol.** 2004

**Pages** 6

**Date accessed** May 15, 2013

**Link/location** ACM

- This paper discusses in-depth a particular way of preventing the user from cheating by withholding unneeded information.
- The increased load on the server and load on the client’s CPU is cited as the primary reason why this is not implemented.
- The author suggested a compromise where a semi-on-demand state dissemination strategy based on the information that the user is likely to require, but this created much of the same weakness that preloading has.

McGraw, Gary, Hoglund, Greg

**Title:** Online Games and Security

**Periodical / event:** Attack Trends

**Vol.** 2007

**Pages** 4

**Date accessed** May 26, 2013

**Link/location** IEEE Security and Privacy

- McGraw and Hoglund discusses in brief the motivation and trend that online cheating is driven by.
- In modern online games, the game world is so big that sharing state information with thousands of clients provides the primary architectural challenge, which leads to deficiencies and allow state confusion attacks.
- Race conditions is discussed where different software states are not synchronized in real time or different databases are accessed by different functions and updates are not necessarily updated in real time.
<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Conference</th>
<th>Year</th>
<th>Volume</th>
<th>Date</th>
<th>Publisher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pierre Louis</td>
<td>- Trust in client software to manipulate state is a requirement for the game to function, but limitation needs to be in place so the user cannot manipulate the software to attack state vulnerabilities. - Pierre Louis discusses some areas that must be considered while attempting to prevent cheating such as preserving real-time quality and privacy issues. - The consequences of false positives and false negatives (Type I and II errors), and how this is currently the most detrimental factor in anti-cheat implementation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Woo, Jiyoung and Kim, Huy Kang</td>
<td>Survey and Research Direction on Online Game Security</td>
<td>WASA 2012</td>
<td>2012</td>
<td>7</td>
<td>May 18, 2013</td>
<td>ACM</td>
</tr>
<tr>
<td>Yan, Jeff and Randell, Brian</td>
<td>A Systemic Classification of Cheating in Online Games</td>
<td>NetGames ’05</td>
<td>2005</td>
<td>9</td>
<td>May 18, 2013</td>
<td>ACM</td>
</tr>
<tr>
<td>Yan and Randell</td>
<td>- Significant opportunities exist to profit illegally as appropriate countermeasures are not developed as quickly as bugs and loopholes are found. - The growth in the gaming industry is not followed by development in anti-cheat mechanism to the same degree, and as it becomes more mainstream, becomes a more important concern than ever. - Provides a clear framework of major threats and countermeasures that are currently available, as well as provide examples of these countermeasures and their limitations. - Major threats are divided by method of attack and while there are effective countermeasures, they are often intrusive on the legitimate user, making it impractical.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This paper is widely cited as a very important piece of work, by using the three identified categories, Yan and Randell was able to provide a framework with which all existing cheats can be categorized and further research on specific types of cheating builds upon this.
Works Cited


Van Der Merwe, Alta, Marianne Loock, and Marek Dabrowski. "Characteristics and Responsibilities Involved in a Phishing Attack." *Characteristics and Responsibilities... Preview & Related Info*. ACM,
