Security Issues in Massively Multiplayer Online Games

ACC 626 Research Paper

Debbie Jiang

6/30/2011

Executive Summary

The massively multiplayer online gaming (MMPG) industry has experienced tremendous growth over the past decade. The number of players, game operators, game designers, and gaming companies with stake in this industry has also increased remarkably. As a result, the need for security in MMPGs is becoming increasingly critical. This paper discusses a variety of security issues which transpired in the world of MMPGs, as well as the methods in which hackers commit frauds. It will then recommend security mechanisms which can prevent and detect these frauds and security breaches.

Cheating, virtual frauds, and other security attacks are becoming increasingly widespread in the virtual world. This is partially due to the extensive amount of wealth that can be extracted from within the games. Users have developed illegal methods to obtain virtual wealth and in turn, convert them into real wealth in the real world. Another factor contributing to the substantial number of security issues is the lack of regulations in this industry. It is extremely difficult to impose legislation in a world that is virtual, and thus "not real". Despite this, it is still vital for game companies to make an effort to ensure that MMPGs are enjoyable and fair for all players. It is also the game company's responsibility to protect players from any unauthorized access to players' personal information.

The first type of security breach issue described in this paper is an attack relating to compromising players' account. Through the usage of malicious software, Trojan horses, social engineering, dictionary and brute force attacks, and exploitation of lack of authentication, a hacker can obtain a player's user name and password in order to obtain his or her virtual wealth. The second type of security issue discussed is a massive data breach, in which the PlayStation Network Outage in April 2011 will be used as an illustration. The third security breach relates to "virtual money laundering", particularly through the usage of tools known as "bots". The fourth common attack on MMPGs is a distributed denial of service attack, in which the attacker attempts to make the game unavailable to players through techniques such as overloading the game server. The last security issue discussed is an internal misuse, in which a game operator uses his or her authoritative power in the game to gain an unfair advantage.

Mechanisms to mitigate the security risks in MMPGs include the usage of dynamic passwords, educating players and game operators, building strong game servers to withstand certain attacks, ensuring an adequate two-way authentication system, automated tests to ensure a human is at the keyboard, and stronger punishments for individuals guilty of security breaches.

Table of Contents

1.0 Introduction

Ever since the first computer game, Tic-Tac-Toe for Electronic Delay Storage Automatic Calculator, was created in 1952 by A.S. Douglas, the gaming market have been growing rapidly, ranging from standalone games on a PC, to the more recent popularization of MMPGs. Due to massive improvements in Internet connectivity over the past 15 years, the number of individuals participating in online gaming has grown extensively. In 2006, it was estimated that there are more than 10 million people playing MMPGs, with the number doubling every two years[1]. One of the most popular MMPGs is Blizzard's World of Warcraft (WoW), which reached a subscriber base of 12 million in October 2010[2].

MMPGs are games where a large number of players interact together in a complex online world. Online or virtual worlds are "game like" environments where players can cooperate and socialize with one another, and also engage in entertainment, education, and other commerce[3]. MMPGs are played on central server clusters (called realms), in which players gain access to the game by connecting their computers over the Internet1. Furthermore, these games are played in massively distributed systems, with thousands of client processes interweaving on a common server, over the network, in real time. Due to the architecture of MMPGs and the large number of participants, there is an inherent lack of security in these games, which creates fertile grounds for cheating1.

In addition to the inherent security risk, MMPGs are also lacking in terms of legal regulation, security and privacy protection, and other related legislation which can resolve these security issues. As a result, users have taken advantage of this shortcoming and exploited these games through hacks, attacks, and cheats. There are couple of obvious motives for hackers to exploit online games. First, games such as WoW have a very sophisticated virtual economy, which gives hackers the opportunity to gain financially by exchanging virtual assets for real assets. Some analysts have argued that the amount of money that can be made in these virtual economies rivals the size of small countries1. Second, game developers did not design gaming software with security as a top priority. Specifically, the massively

[1] Greg Hoglund and Gary McGraw, *Exploiting Online Games: Cheating Massively Distributed Systems* (Boston: Addison Wesley Professional, 2007).

[2] Blizzard Entertainment, "World Of Warcraft® Subscriber Base Reaches 12 Million Worldwide," Blizzard Entertainment, accessed June 26, 2011, last modified October 7, 2010, http://us.blizzard.com/en-us/company/press/pressreleases.html?101007.

[3] Brian E. Mennecke et al., "Second Life and Other Virtual Worlds: A Roadmap for Research," *International Conference on Information Systems 2007* (2007): page 2, accessed June 26, 2011, http://www.bus.iastate.edu/mennecke/CAIS-Vol22-Article20.pdf.

distributed client-server architecture is abundant with vulnerabilities[4]. This creates opportunities for hackers to exploit the security weaknesses inherent in MMPGs.

2.0 The Need for Security

It is obvious why security is needed in the real world, as citizens in society need to be protected against danger, damage, loss, and crime. One may argue that since the virtual world is just a game, what is the incentive for securing it? The rationalization comes from the large number of investors, creators, publishers, and other individuals with large stakes in the game companies. Therefore, it becomes imperative to ensure a game's security safety and ultimately, its financial success. If a particular game is susceptible to cheats, and other security issues, it is unlikely to enjoy financial success as players would simply quit and turn to another game. Additionally, the privacy of players and game operators must be protected in accordance to Personal Information Protection and Electronic Documents Act (PIPEDA)4.

This report will discuss a number of security issues associated with MMPGs. Specifically, it will address how hackers violate security to create cheats, as well as make recommendations on security mechanisms to prevent fraud and security issues. In order to reduce the occurrence hacking and cheating in MMPGs, game developers must begin by becoming more aware of the problem and design games with security in mind.

3.0 Attacks Relating to Compromising Accounts

3.1 Trojan and Other Malicious Software Attacks

MMPGs are common victims of Trojan and malware attacks. WoW is a good example of this type of attack as it is popular among hackers due to the extensive amount of real money involved in the game. Hackers create and plant Trojan horses and malware programs on players' computers in order to obtain user names and passwords. This will enable them to gain access to the virtual gold in players' accounts and sell them in the real world for real money. The Trojan horse programs are often hidden in public computers in Internet Cafes in order to illegally obtain players' usernames and passwords[5]. Below are some examples of such Trojan and malware attacks which targeted WoW.

In September 2006, WoW was victim to a key stroke logging incident, which is designed to track the keys struck on a keyboard such that the keyboard user is unaware that what they type is being monitored. Hackers did this by installing malware in certain websites that is designed to steal user names

[4] Rens van Summeren, "Security in Online Gaming" (unpublished essay, January 26, 2011), accessed June 26, 2011, http://www.cs.ru.nl/bachelorscripties/2011/ Rens_van_Summeren___0413372___Security_in_Online_Gaming.pdf.

[5] Ying-Chieh Chen et al., "Online Gaming Crime and Security Issue – Cases and Countermeasures from Taiwan," *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*: page 131, accessed June 26, 2011, http://dev.hil.unb.ca/Texts/PST/pdf/chen.pdf .

and passwords. Any users who accessed these websites would have been infected through malicious browser pop ups. There was a significant number of WoW players affected by this attack, and as a result, were unable to gain access to their accounts as their username and/or passwords had been changed[6].

Another instance of malware attack on WoW accounts occurred in April 2007 when hackers took advantage of a flaw in the way that Windows dealt with animated cursors, which enabled them to invade users' computers and hack into their WoW accounts. Hackers did this by hosting codes in "maliciously constructed" websites that were used to take over vulnerable computers. This incident also disrupted other MMPGs, but WoW was affected to the greatest extent due to the real money involved. Hackers were then able to sell these WoW accounts to third parties, which were worth at least $10. This amount was massive, since a credit card account at the time was worth only $6 in the market[7].

3.2 Social Engineering

Another method that hackers often resort to in order to obtain MMPG users' usernames and passwords is through social engineering. To carry out this attack, hackers pose as an authoritative figure, such as a system administrator, to scam players into disclosing their usernames and passwords[8]. Some scamming methods include tricking honest players into believing that an attractive or annoying event has happened to their account, thus requiring their username and password. The hacker may notify a player that he or she has won an in-game prize, and login information is required in order to access the reward. In an example, the hacker posing as a system administrator approaches a player, and informs him or her that there is evidence of the player performing certain illegal acts that is against game policy. If the player does not verify his or her login details within a certain time frame, the account will be suspended4.

3.3 Dictionary Attacks and Brute Force Attacks

Dictionary attacks require the hacker attempting every single word in the dictionary in order to determine the password of an account[9]. This attack is effective in taking advantage of users who choose poor and easy to remember passwords (words in the dictionary). This attack may have been effective in the past, but nowadays, passwords are required to be alphanumeric. Brute force attacks involve attempting every single possible character and combinations of characters until the correct sequence is

---

[6] John Leyden, "Warcraft gamers locked out after Trojan attack," *The Register*, September 26, 2006, accessed June 26, 2011, http://www.theregister.co.uk/2006/09/29/warcraft_trojan_attack/.

[7] BBC News, "Cursor hackers target WoW players," *BBC News*, April 5, 2007, accessed June 26, 2011, http://news.bbc.co.uk/2/hi/technology/6526851.stm.

[8] Joel Zetterström, "A Legal Analysis of Cheating in Online Multiplayer Games" (unpublished essay, March 2005), accessed June 26, 2011, http://gupea.ub.gu.se/bitstream/2077/1948/1/200528.pdf.

[9] Tech-FAQ, "Dictionary Attack," Tech-FAQ, accessed June 26, 2011, http://www.tech-faq.com/dictionary-attack.html.

found in order access the account[10]. These attacks are common if the game's authentication system does not have sufficient protection against this4.

3.4 Exploiting Lack of Authentication

To minimize attacks due to compromised accounts, a game should have adequate two-way authentication between both the client and the server[11]. If the two-way authentication is not genuine, a hacker can set up a bogus game server in order to collect user names and passwords from legitimate players (the client). A situation where adequate authentication is required is during a password change request. It is necessary to re-authenticate a player upon a password change request. There could be instances where a player forgets to log off his or her account, allowing another person to have temporary access to that account. Re-authentication would ensure that the person requesting the change is the actual owner of the account.

3.5 Recommendations

In order to prevent and decrease the amount of future malicious attacks and Trojan horses from taking over MMPG accounts, actions need to be taken to improve user authentication. Although the static user name and password authentication method is one of the most simple and lost cost authentication alternatives, it is not the most effective method to secure players' personal information and virtual assets. Another option to protect players would be the establishment of a dynamic password system, which limits a password to be valid only for a one-time use. The motive is to prevent hackers from re-using a compromised password. So even if a hacker was able to obtain a player's username and password through the means of a malicious attack, he or she would not be able to use the login information again. The idea of the one-time password is to integrate the usage of a small hand-held device, which synchronizes the target system's authentication scheme, and displays the one-time password to the player on that device. Furthermore, this one-time password will periodically change. In order to access the account, the user will enter his or her username, password, and the one-time password displayed on the hand-held device. Without the one-time password, the hacker would never be able to gain access to the hacked account[12].

In June 2008, Blizzard unveiled its Blizzard Authenticator to WoW players. The design of this authenticator is essentially the same as a dynamic password. Blizzard began by selling authentication

---

[10] Tech-FAQ, "Brute Force Attack," Tech-FAQ, accessed June 26, 2011, http://www.tech-faq.com/brute-force-attack.html.

[11] Jianxin Jeff Yan and Hyun-Jin Choi, "Security Issues in Online Games," *The Electronics Library* (2002): page 6, accessed June 26, 2011, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.8270&rep=rep1&type=pdf

[12] Ying-Chieh Chen et al., "Online Gaming Crime and Security Issue – Cases and Countermeasures from Taiwan," *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*: page 135, accessed June 26, 2011, http://dev.hil.unb.ca/Texts/PST/pdf/chen.pdf .

devices to its users, and then released a mobile version a year later. The authentication device produces an 8 digit code every 15 seconds that is valid for login within the next 2 minutes. The user would need to enter this code in addition to his or her username and passwords in order to access their account. However, even with such security measures, attackers still discovered a method to breach this system in February 2010. What they did was use a "man-in-the middle attack" method in which they installed a file on a player's computer in order to incept not only the user name, password, but also the 8 digit code. For the moment being, the attacker can use the 8 digit code during the small window of time that it is still valid. To combat this breach of security, as stated in the recommendation above, the generated security code should only be able to be used once4.

In addition to the above recommendation, it is also crucial for MMPG users to be educated about online gaming security. In particular, the responsibility of keeping their username and passwords known only to themselves is essential. Creating security awareness to players is the easiest and least costly of methods to help prevent and minimize the effects of cybercrime. It is simply a matter of gathering all the security information known to game operators and players and distributing them to make available to all players. Forum topics relating to security issues should be highlighted to players. Daily security tips can also be displayed on login pages to serve as reminders to players[4].

Other alternatives to help eliminate and prevent compromising account attacks are to perform online scanning every time players launch their gaming system. This scan will help to detect any Trojan horses or malicious software that could compromise a user's username and password information. However, the effectiveness of this alternative is limited as most hackers are often one step ahead of online scanning software. Many hackers are devoted to building malicious software that online scans are unable to detect. Although not completely effective, the usefulness of the scans should still be maximized through frequent updates to the scanning system[12].

4.0 An Example of Massive Data Breach - PlayStation Network Outage

In April 2011, Sony's PlayStation Network (PSN), which offers online multiplayer gaming services, suffered one of the largest data breaches in history. On April 20, 2011, 77 million PSN members discovered that the PSN was temporarily shut down, and found themselves unable to access their accounts[13]. Although the attack occurred between April 17 and 19, it was not until April 22 that Sony finally confessed the network outage was a result of an unauthorized external intrusion to the PSN. Sony further clarified the outage was not result of a DDoS attack, but rather appears to be the result of an individual breaking into the network[14]. The intrusion resulted in the unauthorized hacker(s) obtaining

[13] Mark Hachman, "Sony PlayStation Network Down for a 'Day or Two,'" *PCMag*, April 21, 2011, accessed June 26, 2011, http://www.pcmag.com/article2/0,2817,2383924,00.asp.

[14] Keir Thomas, "Sony Makes it Official: PlayStation Network Hacked," *PC World*, April 23, 2011, accessed June 26, 2011, http://www.pcworld.com/article/226128/

accounting holders' names, addresses, email addresses, usernames, and passwords. In addition, Sony commented on the possibility that credit card information may also have been compromised. As a precaution, Sony suggested to its users that they "remain vigilant" by investigating their credit card information to determine if there is any evidence of identity theft or financial fraud. Furthermore, Sony hired the Federal Investigation Bureau (FBI) in San Diego to investigate the matter[15].

A week after the initial outage, Sony released another bombshell to the public declaring that users' personal information such as addresses, user names, and passwords were not only stolen during the intrusion, but they were also not encrypted. Sony had only taken action to encrypt users' credit card information. In the week following, Sony disclosed that 2,500 customer names and partial addresses had been posted on a Sony Website by the hacker. These names were obtained from a list of customers who participated in an online sweepstake in 2001. Sony removed the names shortly after it was posted and defended themselves by announcing that the Sony website was old and "inactive"[16]. After the incident, Sony assured the public that "access to its data had been restricted both physically and through the perimeter and security of the network"[17]. After the intrusion, Sony made an announcement encouraging its users to change their passwords[18]. This resulted in the exploitation of another flaw of Sony's PSN system. In order for users to change their PSN account passwords, he/she would only need to provide their email address and birth date, which then created an opportunity for hackers to capture many players' accounts. As a result of this exploitation, Sony had to temporarily disable PSN sign-ins on May 18, 2011[19].

Although it is still unclear how the hack of PSN occurred, there have been a number of speculations. One plausible explanation was that the network intrusion was a result of retaliation from Sony Online Entertainment (SOE) employees who were let go at the end of March. These employees used their access to hack the system as a form of revenge. Another explanation was accusations against PSN's unpatched servers. Individuals claimed that PSN's ran outdated versions of Apache and Linux on their webservers. There were also discussions that the rest of PSN's servers also have not been patched

---

sony_makes_it_official_playstation_network_hacked.html.

[15] Bilton, Nick. "Sony Says PlayStation Hacker Got Personal Data." *The New York Times*, April 26, 2011. Accessed June 26, 2011. http://www.nytimes.com/2011/04/27/technology/27playstation.html.

[16] "Sony: More testing needed before PlayStation relaunch," *Tehran Times*, May 9, 2011, accessed June 26, 2011, http://www.tehrantimes.com/index_View.asp?code=240220.

[17] Chris Griffith, "PlayStation users' personal data not encrypted: Sony," *Australian IT*, April 28, 2011, accessed June 26, 2011, http://www.theaustralian.com.au/australian-it/playstation-users-personal-data-not-encrypted-sony/story-e6frgakx-1226046284120.

[18] Chloe Albanesius, "PlayStation Network Log-Ins Down After Reported Password Exploit," *PCMag*, May 18, 2011, accessed June 26, 2011, http://www.pcmag.com/article2/0,2817,2385557,00.asp.

[19] Chloe Albanesius, "PlayStation Network Maintenance Takes Down Password, Account Access," *PCMag*, May 24, 2011, accessed June 26, 2011, http://www.pcmag.com/article2/0,2817,2385825,00.asp.

for the past five years[20]. There was also much speculation that the hacker group Anonymous were involved as they admitted to a series of DDoS attacks on Sony shortly prior to the massive data breach in April.

Sony suffered tremendously as a result of the massive data breach. A week after the initial network outage, Sony was plastered with a class action lawsuit for the data breach that affected 77 million users worldwide[21]. In addition, Sony was also accused of not alerting their users of the data breach until almost one week after the initial discovery of the incident[22]. To minimize its reputation damages and potential financial losses, Sony immediately took action to offer free content to its users once PSN reopens. Sony proceeded to improve its security systems by boosting its level of data protection and increasing the amount and quality of encryption it uses[23]. Sony also initiated identity theft protection systems to its users[24]. After performing extensive testing on its system, it was not until 23 days after the initial attack, that Sony finally fully restored PSN[24].

4.1 Recommendations

There have been many criticisms relating to the manner that Sony handled the massive data breach incident. First, it took almost an entire week for Sony to notify its users of the data breach. This means that PSN users were completely unaware that their personal information was in the hands of a hacker for almost 7 days. Sony should have announced the server intrusion to its users immediately following its occurrence. This would give users ample time and opportunity to take action and investigate potential identity theft and credit card fraud, which would minimize the potential negative impact of the situation. Second, the lack of encryption on PSN users' personal data was also a wrongdoing on Sony's part. As a result of this, the hackers were able to make use of the personal data as they were readable, and potentially use this information to engage in identity theft. Sony's inaction could have a severe negative impact on the MMPG industry as a whole. As a result of the massive privacy breach, in the future, many users may be hesitant to participate in multiplayer online gaming.

---

[20] John Leyden, *The Register*, May 13, 2011, accessed June 26, 2011, http://www.theregister.co.uk/2011/05/13/veracode_playstation_hack_analysis/.

[21] "PlayStation data breach lawsuit filed," *CBC News*, April 28, 2011, accessed June 26, 2011, http://www.cbc.ca/news/technology/story/2011/04/28/ technology-sony-playstation-data-breach-lawsuit.html.

[22] "Gamers sue Sony over PlayStation hack," *ABC News*, April 29, 2011, accessed June 26, 2011, http://www.abc.net.au/news/stories/2011/04/29/3203512.htm?section=world.

[23] Isabel Reynolds, "Sony to resume some PlayStation services; apologizes," *Reuters*, May 1, 2011, accessed May 1, 2011, http://in.reuters.com/article/2011/05/01/idINIndia-56692820110501.

[24] Mark Hachman, "Sony: (Almost) All PlayStation Network Services Online by Week's End," *PCMag*, May 31, 2011, accessed June 26, 2011, http://www.pcmag.com/article2/ 0,2817,2386167,00.asp.

5.0 Security Issues Relating to Virtual Assets

5.1 Virtual Economy

Virtual economies are becoming an integral part of MMPGs and even in real life. MMPGs create different types of virtual currencies which vary from game to game. The virtual currencies can be used in the game to purchase items for players' avatars, which enhances their chances of winning the game[25]. In the MMPG Second Life, created by Linden Lab, the virtual currency is Linden dollars. Not only can the Linden dollars be used to purchase items such as clothes for players' avatars, and virtual building designs, it can also be exchanged for real US dollars and vice versa. In fact, the currency is so popular that the estimated daily transaction is equivalent to $1 million USD[26]. Due to the large amount of money involved in the virtual world, players often lose interest in actually playing these games. Instead, they view MMPGs an excellent money laundering opportunity, and resort to developing methods to retrieve wealth out of these games. Consequently, some players are inclined to cheat and hack for financial gain[27]. Unfortunately, this frequent lack of gamesmanship eliminates the "fun" for players who are actually devoted to playing.

In WoW, the currency used is virtual gold. This is earned by game advancing activities such as killing in-game enemies. The gold can then be used to improve his or her character and advance further in the game[28]. Some players feel that they are lacking in terms of skill level and do not wish to devote extensive amounts of time in progressing themselves in the game. As a result, they often resort to using real currency to purchase virtual currency. This created the demand for virtual gold and eventually a market for "gold farming", where companies employed "bots" to acquire virtual currency and then sell it in the real world for real currency. Although this practice is a form of cheating and hence against game policy, it is still occurring in the world as there are companies that exist in China for the sole purpose of "gold farming"[29].

---

[25] Jiankun Hu and Fabio Zambetta, "Security issues in massive online games," *Security and Communication Networks* (2008): page 83, accessed June 26, 2011, http://goanna.cs.rmit.edu.au/~jiankun/Sample_Publication/Gaming.pdf.

[26] Chia Yao Lee and Matthew Warren, "Security Issues within Virtual Worlds such as Second Life," *Australian Information Security Management Conference* (2007): page 143, accessed June 26, 2011, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=ism&se redir=1#search="Security+Issues+within+Virtual+Worlds+such+asSecond+Life" .

[27] Gary McGraw and Greg Hoglund, "Online Games and Security," *IEEE Security & Privacy* (September-October 2007): page 76, accessed June 26, 2011, http://www.cigital.com/papers/download/attack-trends-EOG.pdf.

[28] Stefan Mitterhofer et al., "Server-Side Bot Detection in Massive Multiplayer Online Games," *IEEE Security & Privacy* (May-June 2009): page 18, accessed June 26, 2011, http://iseclab.org/papers/botdetection-article.pdf.

[29] Jiankun Hu and Fabio Zambetta, "Security issues in massive online games," *Security and Communication Networks* (2008): page 84, accessed June 26, 2011, http://goanna.cs.rmit.edu.au/~jiankun/Sample_Publication/Gaming.pdf.

5.2 Botting

Botting is a common form of cheating in online games, where a program is utilized to play the game, resulting in minimal and often no human interaction. Some players may find components of the game inherently boring and repetitive and therefore resort to botting to progress in the game. This allows the player to gain experience points and virtual assets without actually investing any time in playing the game. "Gold farming" companies often use botting to earn virtual currencies, and then in turn, sell them in the real world. Consequently, this creates a large supply for virtual currency and causes inflation in the game economy[30]. Players who do not engage in cheating are harmed as their virtual currencies will decline in real value.

Presently, Blizzard devised a program for WoW called Warden, which is a tool designed to detect bot programs. This application runs on players' computers during every logon. While players are engaged in the game, Warden will scan for any suspicious programs such as bots and debuggers. If any of these programs are identified, Blizzard will be informed, and then they will take necessary actions to suspend or ban guilty players' accounts. Warden's effectiveness is limited as it only has the capability to check for known bots. In other words, the program will always be a step behind since bot writers are constantly designing bots that are undetectable by Warden. On top of this, a number of players have already found methods to get around the Warden scan. For instance, if a player logs in as a guest in an administrator account, Warden would not have the authorization to access the account processes[28]. In addition to the above shortcomings, Warden has also been criticized and protested against regarding invasion of privacy4. One of the only other known techniques to detect bots is through human interaction. Players have the capability to report suspicious activities of other players to a game moderator. The moderator, disguised as a player in the game, will approach the suspicious character and attempt to initiate a conversation to determine whether there is a human present at the keyboard[30]. Although this method may sometimes be effective, it is very inefficient. There are millions of online game players, making it impossible to detect all the bots.

5.3 Recommendations

There are a couple of techniques to detect and deter bots that are much more adequate in terms of practicality and efficiency compared to the existing measures described above. One method to detect bots is employing the use of automated tests throughout the game, which is designed to distinguish whether a humans or a computer is at the keyboard. These tests would be designed so that most humans would have the skills and knowledge to pass, but a computer would not. Tests such as simple Math

---

[30] Stefan Mitterhofer et al., "Server-Side Bot Detection in Massive Multiplayer Online Games," *IEEE Security & Privacy* (May-June 2009): page 19, accessed June 26, 2011, http://iseclab.org/papers/botdetection-article.pdf.

problems would be generated, and presented to players when they log onto the game, and then graded subsequently. These tests will then be repeated during random intervals to the players while they are in the game[31]. After a player fails these tests a certain number of times, his or her account would be flagged as suspicious. The moderator should then approach the players with suspicious accounts and through human interaction, determine if there is a human at the keyboard. Accounts in which there is no human would then be banned or suspended permanently.

Often, simply detecting bots is not sufficient, as the exchange from virtual currency to real currency could be almost instantaneous (eBay auctions can take as little as a few hours). Consequently, even when a bot is detected, a substantial amount of virtual and real currency could have already been "laundered". To avoid this, game designers can create a delay for in-game transfer of currency and increase the amount of time to "ship" virtual resources. This would ensure a greater amount of time to allow detection for bots and prevent any unwarranted money transfers from occurring[32].

6.0 Distributed Denial of Service Attacks

6.1 Grey Goo Attack

Distributed Denial of Service (DDoS) attacks are common security issues in MMPGs. One of the most notable occurred in November 2006, when the game Second Life was plagued with what was known as a "grey goo attack". This attack involved the use of "golden ring-shaped virtual objects", which constantly self replicated and flooded across various Second Life locations. The term "grey goo attack" was coined due to its similarity to the self replicating nanotechnology robots that devour physical resources[33]. This attack interrupted many players' game play as avatar clothing vanished, in game teleportation capabilities were disabled, and unreliable account balances were displayed[34]. Furthermore, this DDoS service attack consumed server processor cycles and network bandwidth which left Second Life servers responding slowly[34]. It can be argued that Linden Lab gave hackers the opportunity and the tools to initiate such attacks since they do not approve virtual objects before players submit them into the Second Life world. Players have the ability to create reproducing pets, flowers that spread, and

[31] Philippe Golle and Nicolas Ducheneaut, "Preventing Bots from Playing Online Games," *ACM Computers in Entertainment* 3, no. 3 (July 2005): page 3, accessed June 26, 2011, http://www2.parc.com/csl/members/nicolas/documents/CIE-Bots.pdf.

[32] Philippe Golle and Nicolas Ducheneaut, "Preventing Bots from Playing Online Games," *ACM Computers in Entertainment* 3, no. 3 (July 2005): page 9, accessed June 26, 2011, http://www2.parc.com/csl/members/nicolas/documents/CIE-Bots.pdf.

[33] Chia Yao Lee and Matthew Warren, "Security Issues within Virtual Worlds such as Second Life," *Australian Information Security Management Conference* (2007): page 148, accessed June 26, 2011, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=ism&se redir=1#search="Security+Issues+within+Virtual+Worlds+such+asSecond+Life".

[34] Robert Lemos, "Second life plagued by 'grey goo' attack," *The Register*, November 24, 2006, accessed June 26, 2011, http://www.theregister.co.uk/2006/11/24/secondlife_greygoo_attack/.

attachable objects for their avatars without any approval. However, Linden Lab stated that this is their attempt to make the game as fun as possible for its players since it encourages creativity and innovation[34]. Linden Lab detected this DDoS attack within fifteen minutes of its outbreak and immediately took action to clean out its servers. Although servers were able to return to normal within two hours, this incident was still an exhibit which displayed the susceptibility of this game to viral attacks[33]. Additionally, Second Life's vulnerability to DDoS attacks was further emphasized since the "grey good attack" was its third major attack in less than one year, all of which related to rapidly reproducing digital objects. As a result of these attacks, Linden Labs enhanced its response tools by making its systems more robust. It also implemented limits on how fast objects can replicate, and placed boundaries ("grey goose fence") on regions where replication are allowed to take place.

6.2 Griefing Attack

Another type of DDoS attack, known as a "griefing attack", plagued WoW players in September 2005. "Griefing attack" is a type of bullying, vandalism or harassment by the attacker to the victimized game player. "Griefers" takes advantage of weaknesses and loopholes in the game in order to attack avatars, virtual locations, organizations and events. When these "griefers" visit virtual locations, they attach a computing-intensive object to their avatars, which then overloads the servers of the game. In September 2005, a digital disease spread beyond its intended area in WoW. Malicious players created a monster with the ability to curse in-game avatars with a self-propagating disease. This monster was only intended to transmit the disease to avatars that it is fighting. However, "griefers" quickly took advantage of this tool, and discovered methods to spread the disease all over the WoW world, which resulted in massive casualties and inhabitable cities[35].

6.3 Other DDoS Attacks

In early 2010, one of the European WoW servers was experiencing significant disconnectivity issues. It was later determined that a single player was responsible for overloading the server by abusing an in-game macro4. A more recent DDoS attack occurred in June 2011, where the indie game "Minecraft" and the massively-multiplayer online space game "EVE Online" were victims. A hacker group known as LulzSec was responsible for disabling the logins for Minecraft, and taking down the servers for EVE Online[36].

[35] Robert Lemos, "Digital plague hits online game World of Warcraft," *SecurityFocus*, September 27, 2005, accessed June 26, 2011, http://www.securityfocus.com/news/11330.

[36] Matt Clark, "'Minecraft,' 'EVE Online,' And The Escapist Suffer Denial-Of-Service Attacks," *MTV Multiplayer*, June 15, 2011, accessed June 26, 2011, http://multiplayerblog.mtv.com/2011/06/15/minecraft-eve-online-and-the-escapist-suffer-denial-of-service-attacks/.

6.4 Recommendations

DDoS in MMPGs are extremely difficult to prevent and stop since the attack could be coming from many sources. What the game developer companies can do is to build infrastructure for several times greater than what the normal peak traffic of the game is expected to be. The server bandwidth should also be flexible enough to withstand certain DDoS attacks. A monitoring system should also be implemented to ensure the smooth operations of servers and other infrastructure[37]. However, this may be impractical due to the immense costs required. Players themselves also should be educated on the attributes of a DDoS and malicious objects to ensure that the virtual world remains cleansed and "disinfected"[38].

7.0 Internal Misuse

Often security threats come from within the game company rather an external party. A type of this is internal misuse, which when game operators, system administrators, and even game developers engage in cheating within the game. Under normal circumstances, a game operator's responsibility is to assist players in the game when they come across certain difficulties. In particular, they aid players who are victims of harassment, and also in some circumstances, have the ability to transport players to any virtual location. Often, this power is misused for personal financial gain or entertainment4, and also for the purposes of gaining an unfair advantage over normal players8. Some examples of cheats that these game operators have engaged in are:

1) Create valuable items in MMPGs and sell them for financial gain8.
2) Conjure any character or weapon they wish to use[39].
3) Acquire compromised passwords using techniques such as dictionary attacks[11].
4) Make modifications to characters for personal use or another player for a fee[40].
5) Collusion between game operator and dishonest player in order to commit a cheat within the game4.

---

[37] Ram Mohan, "How to Defend Against DDoS Attacks," *SecurityWeek*, April 27, 2010, accessed June 26, 2011, http://www.securityweek.com/content/how-defend-against-ddos-attacks.

[38] Chia Yao Lee and Matthew Warren, "Security Issues within Virtual Worlds such as Second Life," *Australian Information Security Management Conference* (2007): page 147, accessed June 26, 2011, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=ism&se redir=1#search="Security+Issues+within+Virtual+Worlds+such+asSecond+Life".

[39] Jianxin Jeff Yan and Hyun-Jin Choi, "Security Issues in Online Games," *The Electronics Library* (2002): page 6, accessed June 26, 2011, http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.99.8270&rep=rep1&type=pdf

[40] Knut Håkon T Mørch, "Cheating in Online Games - Threats and Solutions," *Norwegian Computing Center/Applied Research and Development* (January 2003): page 8, accessed June 26, 2011, http://www.hackerzvoice.net/ceh/CEHv6%20Module%2051%20Hacking%20and%20Cheating%20Online%20Games/ .

Sometimes, the internal misuse is unintentional. For example, the game operator employee can make an inadvertent mistake by providing a player an item that he should not receive. Although the player was fully aware that he should not be in possession of the item, he does not report this mistake. An instance of this was in the game WoW, where a dishonest player came in possession of an item that allowed him to destroy any hostile unity approaching him. Instead of reporting this mistake, he proceeded to "kill his way through the game"4. His action resulted in permanent suspension of his account and was also ultimately banned from the game4.

7.1 Recommendations

Internal misuse is very difficult to prevent as game operators must be given certain privileges in order to perform their responsibilities. However, a detection technique could be to keep a log of all privileged operations taken by game operators. Every time an item is given by the game operator to a player, the event should be documented in a log. The log should include what item was given, as well as why it was given. The log could be a source of evidence used to catch cheaters. There should also be an agreement that game operators must sign at the beginning of their employment stating that their actions on their job would be free of cheating. In addition, those who engage in activities that gives them an unfair advantage should severely punished. This imposes a high risk and disincentive on those game operator employees who wish to engage in cheating.

8.0 Conclusion

The prevalence of security issues in the online gaming industry is primarily due to the inherent security risks in the virtual world. Online game companies have definitely made substantial efforts to correct their past mistakes and effectively combat security attacks. Since the most common type of attack in MMPGs is related to compromised accounts, much of the remaining responsibility in securing virtual worlds falls to the players themselves to keep their user name and passwords confidential and acquire knowledge on MMPG security.

Annotated Bibliography

1	Hu, J., & Zambetta, F. (2008). Security Issues in Massive Online Games. *Security Comm. Networks*, 83-92. Retrieved from http://goanna.cs.rmit.edu.au/~jiankun/Sample_Publication/Gaming.pdf **Annotation** This paper classified online cheating into two classes. The generic class comprises of eight types of cheating, while the 'of special relevance' class includes cheating that is either occurring in online games or is exhibiting some interesting features in the context of online games. The paper then outlines means of addressing cheating for the following: Generic class 1) Denying service to peer players 2) Compromising passwords 3) Exploiting lack of secrecy 4) Exploiting lack of authentication 5) Exploiting a bug of design loophole 6) Compromising game servers 7) Internal misuse 8) Social engineering Of special relevance to online games 1) Exploring misplaced trust 2) Collusion 3) Abusing the game procedure 4) Relating to virtual assets 5) Exploiting machines intelligence 6) Modifying client infrastructure 7) Timing cheating

2	McGraw, Gary, and Greg Hoglund. "Online Games and Security." *IEEE Security & Privacy*, September- October 2007, 76-79. Accessed May 30, 2011. http://www.cigital.com/papers/download/attack-trends-EOG.pdf. **Annotation** Sophisticated hackers worked in the field of MMORPGs for years; some make a living directly from cheating at gaming. They do this by: 1) Security-related bugs exist 2) Telehacking: a simple state manipulation attack - State machine that manages travel is usually held in the client software. If you alter the client, you can alter the way you travel 3) Using bugs to confuse state boundaries
3	Cikic, Sabine, Sven Grottke, Fritz Lehmann-Grube, and Jan Sablatnig. "Cheat-Prevention and Analysis in Online Virtual Worlds." *1st International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia* (May 2008). Accessed May 30, 2011. http://eprints.physik.tu-berlin.de/204/01/Final_Paper.pdf. **Annotation** The two most common types of main virtual crimes are fraud and cheating: 1) Fraud - Deception to gain virtual property without paying for it - The way trading works in many online games encourages defrauding your trade-partner ○ Sell game items outside of game (eBay), trade good inside game, but fail to receive payment outside of game -> hard to prove that the good was delivered ▪ No logs maintained, no cash vs goods automatic exchange ○ Solution: Sony installed Station Exchange Service 2) Cheating: allows players to do things that he should not be able to do: - Illegal knowledge ○ knowing things that the player is not supposed to know yet (maphacks, wallhacks) ○ Solution: traditional client-server systems -> limiting info flow as tightly as possible; peer to peer systems -> lock-step protocol - Illegal actions ○ Cloning items or generating large amounts of items

4	Kogan, Ilya. "An Analysis of Cheat Prevention in Peer-to-Peer Massively Multiplayer Online Games." June 2010. Accessed May 31, 2011. http://etd.ohiolink.edu/send-pdf.cgi/Kogan%20Ilya.pdf?ouhonors1276273302. **Annotation** Evaluates the various cheating scenarios and prevention techniques in massively multiplayer online games. Cheating methods 1) Event timing and disruption 2) Lack of secrecy 3) Compromised client or infrastructure
5	Chen, Y.-C., Chen, P. S., Song, R., & Korba, L. (2004). Online Gaming Crime and Security Issue - Cases and Countermeasures from Taiwan. *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*, 131-136. Retrieved from http://dev.hil.unb.ca/Texts/PST/pdf/chen.pdf **Annotation** The number of cyber-criminal activities has increased dramatically. The main type of online gaming crime discussed is: - Hackers aim at userID and password as an attack to capture virtual treasures. o Employ Trojan horse programs or cheat code via Email, malicious websites, FTP sites, plug-in software, cheating programs, hide Trojan in public computers of Internet cafe, etc o Prevention: ▪ Static password, digital certificate, smart card, biometric authentication, password transmitted via cell phone, dynamic password authentication
6	Endicott-Popovsky, B., & Weller, A. (2010, May). Securing Virtual Worlds. *SC Magazine*, 54. Retrieved from http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?index=1&did=2058494841&SrchMode=2&sid=1&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306714064&clientId=16746&cfc=1 **Annotation** With the rapid advancement in technology, the pace of people entering the virtual world is much faster than the pace that controls are implemented for these worlds to protect the users. As a result, the number of attacks in the virtual worlds has also grown drastically. - Gaining control of in-world resources or disrupting user experience - Gaining access to real-world resources (user bank accounts) o Usage of small pink box in the game that users cannot resist opening, but contains programs that can remotely manipulate users' computers - Need to heighten user awareness about these scams

7	Lee, C. Y., & Warren, M. (2007). Security Issues within Virtual Worlds such as Second Life. *Australian Information Security Management Conference*, 142-151. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=ism&seredir=1#search="Security+Issues+within+Virtual+Worlds+such+asSecond+Life" **Annotation** The more developed the virtual worlds become, the greater the breaches of security will be as well as the real world. Below are the security issues within the Virtual World of Second Life discussed: 1) Security breach of user details - Hacking attack upon Second Life's database - Data was encrypted, but still risk of identity theft and financial frauds (Second Life users have their credit card info registered 2) "Grey Goo" attack - Worm-like malicious virtual objects appeared at various locations of Second Life Grid 3) Griefing attacks - Large number of attackers swamp a virtual location or event, generating excess avatar traffic 4) Copybot - Application that makes unauthorized copies of virtual objects and avatars 5) Permission request weakness - System can be abused to hide fraudulent and unauthorized monetary transactions
8	Jha, S., Katzenbeisser, S., Schallhart, C., Veith, H., & Chenney, S. (2008, January). Semantic Integrity in Large-Scale Online Simulations. *ACM Journal, 1*(2), 1-23. Retrieved from http://christian.schallhart.net/publications/2010--toit--semantic-integrity-in-large-scale-online-simulations.pdf **Annotation** Attacks against semantic integrity often compromise the physical laws of the simulated world - enabling the users' simulated persona to fly, walk through walls, or run faster than anyone else. Semantic integrity is the property that repeated online experiments should yield the same results regardless of the user. Virtual economies are highly sensitive to attacks against semantic integrity: 1) It is important to enforce identical policies and restrictions on all participants 2) Strong incentive for malicious users to manipulate semantic integrity in order to gain financial profit or other advantages

9	Mitterhofer, S., Platzer, C., Kruegel, C., & Kirda, E. (2009, May/June). Server-Side Bot Detection in Massive Multiplayer Online Games. *IEEE Security & Privacy*, 18-25. Retrieved from http://iseclab.org/papers/botdetection-article.pdf **Annotation** One of the greatest threats that MMPGs face is a type cheating known as botting. Botting is when a person uses a program that can play the game with minimal or no human interaction. This article proposes an automated technique that detects bots on the server side based on character activity, which is also completely transparent to end users. 1) Player reports suspicious characters, then game moderator will try to have a conversation with the character in question 2) Automatically detect bots by focusing on the server side instead of the client side. This approach first processes and transforms a character's movement data before it interprets the results of these steps to expose bots.
10	Portnoy, A., & Rizvi-Santiago, A. (2009, May/June). Walking on Water - A Cheating Case Study. *IEEE Security & Privacy*, 20-22. Retrieved from http://www.cs.tufts.edu/comp/50GD/assignments/msp2009030020.pdf **Annotation** Today, we often see MMPGs written in dynamic languages, such as Python or Ruby. The digression to these dynamic languages is creating unforeseen risks to intellectual property, and makes it easier for malicious users to sabotage the game. 1) Code modification 2) Susceptibility to botting 3) Dynamic recompilation - players can enumerate functions developed in the developer's source code and call those functions themselves eg) create valuable assets
11	Hoglund, G., & McGraw, G. (2007). *Exploiting Online Games: Cheating Massively Distributed Systems*. Retrieved from http://my.safaribooksonline.com/book/programming/game-programming/9780132271912 **Annotation** There are many ways to cheat in an online game. This book introduces and describes some basic cheating concepts: 1) Building a bot 2) Using the user interface (UI) 3) Operating a proxy 4) Manipulating memory 5) Drawing on a debugger 6) Finding the future

12	Yan, J. J., & Choi, H.-J. (2002). Security Issues in Online Games. *The Electronic Library, 20*, 1-13. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.99.8270&rep=rep1&type=pdf **Annotation:** This paper outlined the various types of online cheatings, and introduces security techniques that can deal with these cheatings. Cheating mitigation techniques 1) Built-in cheating detection: automatically detect and prevent cheating behaviours 2) Educate players so they aware of security issues 3) Good password practice and management 4) Fair trading of virtual assets: introduce a trusted third party 5) Bug patching approach 6) Active complain-response channel 7) Logging and audit trail: logging each game as a session record 8) Post detection mechanisms: cheaters should be punished appropriately

Other Bibliography

ABC News. "Gamers sue Sony over PlayStation hack." April 29, 2011. Accessed June 26, 2011. http://www.abc.net.au/news/stories/2011/04/29/3203512.htm?section=world.

Albanesius, Chloe. "PlayStation Network Log-Ins Down After Reported Password Exploit." *PCMag*, May 18, 2011. Accessed June 26, 2011. http://www.pcmag.com/article2/0,2817,2385557,00.asp.

Albanesius, Chloe. "PlayStation Network Maintenance Takes Down Password, Account Access." *PCMag*, May 24, 2011. Accessed June 26, 2011. http://www.pcmag.com/article2/0,2817,2385825,00.asp.

BBC News. "Cursor hackers target WoW players." *BBC News*, April 5, 2007. Accessed June 26, 2011. http://news.bbc.co.uk/2/hi/technology/6526851.stm.

Bilton, Nick. "Sony Says PlayStation Hacker Got Personal Data." *The New York Times*, April 26, 2011. Accessed June 26, 2011. http://www.nytimes.com/2011/04/27/technology/27playstation.html.

Blizzard Entertainment. "World Of Warcraft® Subscriber Base Reaches 12 Million Worldwide." Blizzard Entertainment. Accessed June 26, 2011. Last modified October 7, 2010. http://us.blizzard.com/en-us/company/press/pressreleases.html?10100

CBC News. "PlayStation data breach lawsuit filed." April 28, 2011. Accessed June 26, 2011. http://www.cbc.ca/news/technology/story/2011/04/28/technology-sony-playstation-data-breach-lawsuit.html.

Clark, Matt. "'Minecraft,' 'EVE Online,' And The Escapist Suffer Denial-Of-Service Attacks." *MTV Multiplayer*, June 15, 2011. Accessed June 26, 2011. http://multiplayerblog.mtv.com/2011/06/15/minecraft-eve-online-and-the-escapist-suffer-denial-of-service-attacks/.

Golle, Philippe, and Nicolas Ducheneaut. "Preventing Bots from Playing Online Games." *ACM Computers in Entertainment* 3, no. 3 (July 2005). Accessed June 26, 2011. http://www2.parc.com/csl/members/nicolas/documents/CIE-Bots.pdf.

Griffith, Chris. "PlayStation users' personal data not encrypted: Sony." *Australian IT*, April 28, 2011. Accessed June 26, 2011. http://www.theaustralian.com.au/australian-it/playstation-users-personal-data-not-encrypted-sony/story-e6frgakx-1226046284120.

Hachman, Mark. "Sony: (Almost) All PlayStation Network Services Online by Week's End." *PCMag*, May 31, 2011. Accessed June 26, 2011. http://www.pcmag.com/article2/0,2817,2386167,00.asp.

Hachman, Mark. "Sony PlayStation Network Down for a 'Day or Two.'" *PCMag*, April 21, 2011. Accessed June 26, 2011. http://www.pcmag.com/article2/0,2817,2383924,00.asp.

Lemos, Robert. "Digital plague hits online game World of Warcraft." *SecurityFocus*, September 27, 2005. Accessed June 26, 2011. http://www.securityfocus.com/news/11330.

Lemos, Robert. "Second life plagued by 'grey goo' attack." *The Register*, November 24, 2006. Accessed June 26, 2011. http://www.theregister.co.uk/2006/11/24/secondlife_greygoo_attack/.

Leyden, John. "Security watchers unpick PlayStation hack" *The Register*, May 13, 2011. Accessed June 26, 2011. http://www.theregister.co.uk/2011/05/13/veracode_playstation_hack_analysis/.

Leyden, John. "Warcraft gamers locked out after Trojan attack." *The Register*, September 26, 2006. Accessed June 26, 2011. http://www.theregister.co.uk/2006/09/29/warcraft_trojan_attack/.

Mørch, Knut Håkon T. "Cheating in Online Games - Threats and Solutions." *Norwegian Computing Center/Applied Research and Development* (January 2003). Accessed June 26, 2011. http://www.hackerzvoice.net/ceh/CEHv6%20Module%2051%20Hacking%20and%20Cheating%20Online%20Games/Cheating%20in%20Online%20Games.pdf.

Mohan, Ram. "How to Defend Against DDoS Attacks." *SecurityWeek*, April 27, 2010. Accessed June 26, 2011. http://www.securityweek.com/content/how-defend-against-ddos-attacks.

Summeren, Rens van. "Security in Online Gaming." Unpublished essay. January 26, 2011. Accessed June 26, 2011. http://www.cs.ru.nl/bachelorscripties/2011/Rens_van_Summeren___0413372___Security_in_Online_Gaming.pdf.

Reynolds, Isabel. "Sony to resume some PlayStation services; apologizes." *Reuters*, May 1, 2011. Accessed May 1, 2011. http://in.reuters.com/article/2011/05/01/idINIndia-56692820110501.

Tech-FAQ. "Brute Force Attack." Tech-FAQ. Accessed June 26, 2011. http://www.tech-faq.com/brute-force-attack.html.

Tech-FAQ. "Dictionary Attack." Tech-FAQ. Accessed June 26, 2011. http://www.tech-faq.com/dictionary-attack.html.

Tehran Times. "Sony: More testing needed before PlayStation relaunch." May 9, 2011. Accessed June 26, 2011. http://www.tehrantimes.com/index_View.asp?code=240220.

Thomas, Keir. "Sony Makes it Official: PlayStation Network Hacked." *PC World*, April 23, 2011. Accessed June 26, 2011. http://www.pcworld.com/article/226128/sony_makes_it_official_playstation_network_hacked.html.