RADBOUD UNIVERSITY NIJMEGEN

Security in online gaming

Bachelor Thesis Information Science

Rens van Summeren

January 26, 2011

Online gaming has gone through an explosive growth in popularity during the last decade, and continues to grow at a great speed. With this growth in popularity and thus in the amount of players, the need for security also becomes increasingly clear. This thesis aims to provide a definition of security in online gaming, as well as security analysis for the various threats with examples and countermeasures. The goal is to help players and game developers assess online gaming security, and inform security experts about existing issues.

CONTENTS

1 INTRODUCTION

DEFINITION

In this thesis I will attempt to map the current state of security within and around online gaming. I will look at why certain security measures are required, what issues threaten the security and in which way, and how the security measures or protection methods are being implemented in practice. This leads to the following research question:

> *What is the current state of the security in online gaming?*

PREFACE

As an information science student and an active online gamer I have always been interested about business going on around online games; especially when it comes to security issues both online games (or online game operators) and gamers face. Because of the link of software security and information security with the field of information science, I felt like it was a good idea to write my bachelor thesis on this subject.

Online gaming has undergone an explosive growth in the last decade. Where computer games used to be mainly a single-player activity, an online multiplayer-mode has become standard in most games; some games these days are entirely built around online game play, diminishing or even completely removing offline game play. With this, the amount of online gamers grows. A consequence of online gaming is the introduction of personal gaming accounts for all these players, and thus the issue of authentication shows up. Another issue that rises with the increase in popularity of online gaming is cheating; where players just cheat themselves in single-player games, they suddenly start to cheat on each other and on online game operators.

Some online games introduce digital items and currency for players to accumulate that is tradable between accounts, potentially making accounts very valuable; not just emotional value, but also monetary value. Accounts become wanted objects for cybercriminals, leading to attempts to steal these accounts away from players.
Important aspects of online games, just like much other software, are confidentiality, integrity and availability. How are these aspects threatened by cheating players on one side, and cybercriminals on the other side, and how are these threats addressed by online game operators? I attempt to answer these questions by splitting the research question into five parts, namely:

1. *Why is security required within and around online gaming?*
2. *Which security issues are present within and around online gaming?*
3. *How can these issues be classified and analyzed?*
4. *How do operators of online games protect themselves against these issues?*
5. *How well do these protection methods deal with the security issues, and what problem areas persist?*

Each of the above questions has its own chapter in this thesis in which it is being addressed. I have used available literature to explore the subject, and used my own knowledge from and experience with online gaming to complement the literature.

2 Online Gaming

This chapter describes why the research topic of this thesis is relevant. In section 2.1 I describe why out of all the different software applications games are chosen. Section 2.2 briefly sums up the most well-known types of online games and compares the different business models that are used when deploying an online game. Section 2.3 introduces Massive Multiplayer Online (MMO) games, which are by far the most relevant types of games when it comes to looking at online gaming security and online game security issues, as this section also starts to explain. In 2.4 further explanations about why MMO games are the most relevant for this type of research are given, as well as the reasons security is required here. Section 2.5 then continues on this by taking a look at some characteristics of offenders and their motives.

2.1 Why Look at the Security of Online Games?

As Hoglund and McGraw put it in their book *Exploiting Online Games: Cheating Massively Distributed Systems*, online games 'are a harbinger of technical software security issues to come. Modern software of all kinds (not just game software) is evolving to be massively distributed, with servers interacting with and providing services for thousands of users at once. [..] What we learn [in MMOs] today is bound to be widely applicable tomorrow in every kind of software. Adding to the urgency of the security problem is the fact that online games are big business' [1].

2.2 Types of Online Games and Business Models

Online games are games that are played online mostly over the internet, but also via LAN (local area network) or even telecommunication. Using a broad definition, online gaming includes internet gaming, web gaming (gaming in a web-browser), online gambling, LAN gaming and mobile gaming. To mention a few types of online games, there are sports games, shooters, strategy games, role-playing games and casino games (like online poker).

Developers use different business models to deploy their online gaming services. It is important to take note of the differences as they can sometimes be used to see what security issues are relevant to a specific game and which ones are more or less diminished because of the business model used. The business models also show the differences in how the gaming software developers earn money on deploying and maintaining a game. Chen et al. categorize the business models into three groups [2], I added a fourth one. It is unclear why Chen et al. do not mention these; one explanation could be that this fourth one has only recently become popular as a model to earn money on with the rise in popularity of micropayments.

1. *Charge for software license*
   this is the traditional business model for deployment of computer games, and so it is also used for online games. A customer only pays once for the game, and has unlimited access to the online features for as long as the game (or its most recent version) is being supported. Most non-MMO games make use of this business model; think of sports games, strategy games and shooters. An example of an MMO game utilizing this is NCSoft's Guild Wars.
2. *Charge for network connection*
   sometimes, publishers choose to distribute their client software free of charge. Profit is made from selling a service, as costumers can only play the games by logging onto the

vendors' servers. This tackles a great deal of today's piracy issues, as copyrights on the client software are not much of a problem. Especially in Asia this business model works great as the Asian gamers have never been used to be charged for software licenses for online games.

3. *Charge for software license and network connection*
   in this business model, customers have to buy the game client to play the game, but they also have to pay a monthly fee to access the game servers. This is by far the most used business model for MMO games.
4. *No charge for software license nor network connection*
   Games in this category are mostly web-based arcade games, but also online poker and Second Life fall into this category. Commercial games can sometimes choose to adopt this model: the Lord of the Rings MMO role-playing game recently switched from group 3 above model[1]. Game client as well as server access is free of charge, profit is being made through so-called 'micropayments'; players pay for additional features and functionality to their game. Only a month after the switch, Lord of the Rings Online's publisher Warner Bros Interactive Entertainment announced that revenue has doubled since going free-to-play[2].

I am going to make the distinction between two types of online games in this thesis: *massively multiplayer online games* (*MMOs*), and *other online games*. With *other online games* I mean any online game that is not a MMO, and therefore don't contain a persistent virtual world – think shooters, race games, sports games, strategy games, card games and board games.

2.3 Massive Multiplayer Online Games

MMOs are multiplayer video games capable of supporting a large amount of players at the same time. They are played over the internet and contain one or more worlds that persist regardless of the presence of players. In MMOs, players are able to compete and cooperate with each other, and interact with other people all over the world. The most popular type of MMO is the massive multiplayer online role playing game (MMORPG), and thus this specific type of MMO will be mainly referred to in the rest of this thesis.

Hoglund and McGraw explain why MMORPGs are interesting as a case study in software security: 'MMORPG games are made of very sophisticated software built around massively distributed client-server architecture. [T]hese games push the limits of software technology, especially when it comes to state and time (not to mention the real-time interaction of hundreds of thousands of users) [...].' [1]

Tens of millions of people play computer games all over the world, and according to Microsoft, gaming is the third most common activity on its platform, after browsing the web and checking e-mail. According to a PricewaterhouseCoopers paper from 2008, the video game industry earned $41.9 billion in global sales in 2007, and is expected to grow to $68.3 billion in 2012. The online

[1] http://www.joystiq.com/2010/09/11/psa-lord-of-the-rings-online-now-free-to-play/
[2] http://www.joystiq.com/2010/10/07/lord-of-the-rings-online-doubles-revenue-since-going-free-to-pla/

gaming industry contributes respectively $6.6 billion and $14.4 billion to those numbers.[3] To get an idea of the size and economic impact of MMO games, let's have a look at some numbers [3]:

The total amount of active (paid) subscriptions of MMOs in 2000 was about 1 million. This grew to over 3 million in 2002, then to around 12 million in 2006 and to 16 million in 2008.
In 2004, Blizzard Entertainment released their MMORPG World of Warcraft. By April 2008, it had attained a market share of over 60% (62,2%, April 2008) with close to 10 million active subscriptions. In October of 2010, Blizzard announced to have reached 12 million active subscriptions for their game[4], making it the most successful subscription-based MMORPG in gaming history. To compare: the MMO ranked second, NCSoft's Lineage, peaked just above 'only' 3 million active subscriptions between 2002 and 2004[5]. All of the subscription owners pay roughly 13 euro each month, as well as many one-time payments for additional services such as server transfers, name/sex/race/faction changes of player characters and in-game items. This accounts for €1.9 billion a year, made by just one company, on just one game, only counting subscriptions. Not to mention that all of these gamers paid for the client software as well, often several times as there have been three expansions already (this is not entirely correct as the client software is downloadable free of charge, and the fee is actually being paid for creating and upgrading accounts).

MMORPGs create virtual words in which virtual items come to have value. This value is mostly reflected by the amount of time players spend on the game. Virtual currency is being gathered and traded, and the state of the game world and the player's characters progress over periods of months or even years. The player accounts involved increase in value over time as virtual property is accumulated. Many MMORPGs have a GDP (gross domestic product) that's larger than that of most small countries. *The Walrus* magazine reported in June 2004:

The Gross National Product of EverQuest, measured by how much wealth all the players together created in a single year inside the game, turned out to be $2,266 per capita. By World Bank rankings, that made EverQuest richer than India, Bulgaria, or China, and nearly as wealthy as Russia. It was the seventy-seventh richest country in the world. And it didn't even exist.[6] [7]

The economy of these MMORPGs is directly connected to the real-world economy through various middle market companies. These companies allow for currency exchange and the sale of virtual items, and more generally the monetization of game play. The implication of this is that cheating and hacking can be directly monetized. Game play itself is a weak form of wealth creation because virtual items and experience points have real value. Sweatshops are parallelizing game play to create virtual wealth on a factory scale. In these sweatshops, people in low-wage countries 'farm' in-game currency, experience and items with a value larger than what they're paid. This leads to much activity on the black market surrounding systems to cheat in an undetectable manner. [4]

[3] http://www.reuters.com/article/idUSN1840038320080618
[4] http://us.blizzard.com/en-us/company/press/pressreleases.html?101007
[5] several interesting graphs regarding these numbers can be found on http://www.mmogchart.com/charts/
[6] http://www.walrusmagazine.com/article.pl?sid=04/05/06/1929205&mode=nested&tid=1
[7] http://news.bbc.co.uk/2/hi/science/nature/1899420.stm

2.4 Why is Security Needed?

Some people may think that security isn't a big deal when it comes to online gaming. The security of public locations is a big deal, because some terrorist might bomb it. Security of a store is a big deal, because people might steal stuff, and a similar thing can be said about the security of digital products, such as software, movies and music. Online games are just there for fun and enjoyment, so why is it so important that they are secure as well?

The internet is undergoing an explosive growth, bringing along lots of computer security issues. Online games suffer from these problems directly because of the way they are built (see 2.3). World of Warcraft is interesting to look at for these security issues for three reasons. First of all there is the amount of client-server and real-time interactions going on in its architecture, opening up lots of opportunities to intercept, change, add and remove messages, directly affecting the game. Then there is the economy of World of Warcraft which is huge, and there are many possible ways to transfer real money into and out of the game, as I already discussed in the previous section. Lastly, there is the size of the game's player base. A game this popular, using this architecture and having such a big economy, is extremely attractive for cheaters, hackers and even criminals.

There are many stakeholders in online games, and to their success. There are the players, the game companies with creators and publishers and all investors and other companies involved with the game companies. They all benefit from a game being successful and healthy for a longer period of time. The lifetime of (offline) single player games is only a few weeks to a few months, but successful online games last for years: the real-time strategy game Starcraft was released in 1998 and is still being played at tournaments with huge money prizes (sometimes over $50.000) and only now, 12 years later, its popularity is slowly starting to decline after the release of Starcraft 2 which is in nearly every aspect superior. The online shooter Counter-Strike was released in 1999 and is still one of the most popular shooters at (online) tournaments, despite the literally hundreds of rivaling shooter games released since.

When an online game is successful, players remain loyal to it for a long time. When a game is unfair, and vulnerable to cheats and attacks, players are likely to quit and/or move on to another game (of course a game has to be likeable to attract enough players in the first place). This is where the challenge lies for game companies: keep the game alive by dealing with anything that promotes unfairness and anyone that (intends to) exploit(s) vulnerabilities, as well as repairing these vulnerabilities as fast as possible. All this in order to attract as many players as possible and to keep them playing – and more importantly: paying – for as long as possible. The two first rules Matthew Pritchard introduces in *How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It* apply here:

> ' Rule #1: If you build it, they will come -- to hack and cheat.
> Rule #2: hacking attempts increase with the success of your game. ' [5]

Additionally, there is the privacy of players and operators of a game to be protected. Nobody is interested in having their personal information out in the open, and many players of MMORPGs do not even want their family or (future) employers to know about their playing at all. Moreover, players are often emotionally involved in the game they play. Bad behavior of other players (even cheaters!) can lead to retaliations, so what if everyone can just look up their fellow player's whereabouts to physically harass them, or to blackmail them? In-game embarrassment of your

character could lead directly to you, and cases are known of players committing suicide over social events taking place inside an online game.[8]

Finally, there is the law that relates to cyberspace which is still very much under development. 'The legal implications of exploiting online games change every day, and the cases themselves are incredibly interesting'. [4] This makes it a much better idea to prevent people from cheating, hacking and exploiting than to sue them after they do so.

So security in online gaming is needed for several reasons. First there is the massively distributed client-server architecture (mainly in MMOs) that has a lot of vulnerabilities. Next there is the economy within many of these games, with which real-world profits can be made. Then there are the millions of online gamers who are willing to pay for playing a game for years as long as it remains fair and protects them against each other and outsiders. Lastly, there is the still dodgy law around exploiting online games.

2.5 Who Threaten the Security, and Why?

MMOs are played by people from pretty much all ages, from all over the world, and many different nationalities and cultures come together in online communities. When it comes to characteristics of cheaters, some interesting findings are presented in *An analysis of online gaming crime characteristics*, after analyzing 613 online gaming related criminal cases from 2002 in Taiwan: 'The offenders (95.8 percent) and victims (87.8 percent) are mainly male and offenders always proceed alone (88.3 percent). The age of offenders is quite low (63.3 percent in the age range of 15-20), and 8.3 percent of offenders are under 15 years old. The offenders are mostly students (46.7 percent) and the unemployed (24 percent), most of them (81.9 percent) not having criminal records.'

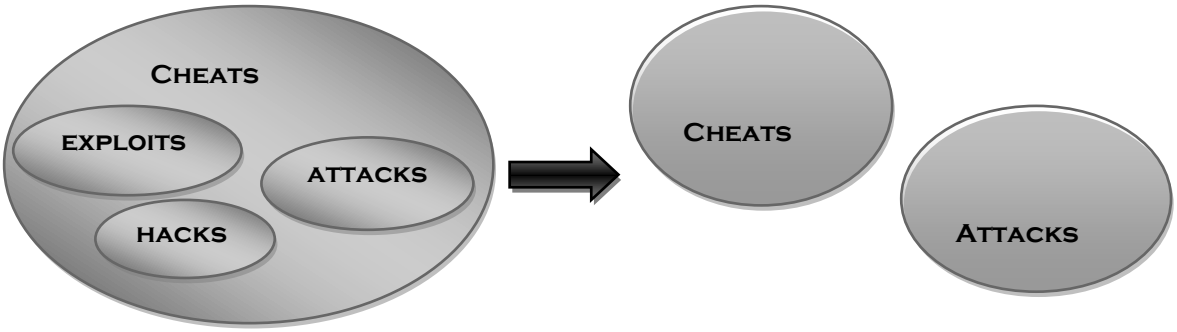
When it comes to cheating behaviors Been-Lirn Duh et al. state that 'little is known about the motives that drive cheaters to cheat.' [6] However, some things can be said about these motives. Just as there are many kinds of honest players, there are many kinds of players who cheat and exploit. The first games were made by classic hackers (before the term *hacker* became a negative one), and because hackers are driven by pushing software to its limits and testing out its possibilities, they were also the first ones to create systems for cheating purposes. Hackers are mainly driven by gaining status and showing off their skill to make a reputation within the clans they are often part of.

Still, there are a lot of people who pose a threat to the security of games that are not directly defined as hackers. Some of them are criminals who make a living out of it, for example by running the previously mentioned sweatshops, or by dealing in stolen account details. Others are legitimate gamers gone bad, or people who cannot or do not want to spend enough time in a game, and buy in-game currency and power leveling services from middle market companies. Sometimes normally honest players even cheat, for example to get early access to new areas of virtual worlds that are already patched into a game, but still off-limits to gamers until they are officially released.

[8] http://articles.cnn.com/2002-04-05/tech/everquest.suicide.idg_1_everquest-sony-online-entertainment-online-game?_s=PM:TECH

3 Security Issues

Until now I have not really talked about various categories of security issues, but simply used the term *cheats*. Other authors use various terms when talking about security issues in online games, such as *hack* (remotely break into computers), *exploit* (take advantage of bugs, glitches and vulnerabilities), *cheat* (playing unfair to gain an advantage), and *attack*, which is the common term to be used when talking about security issues. Often [1,5,7], these four terms are not separately defined, but simply defined as *cheats.* The definition of cheating given by Yan and Randell [7] is: 'Any behavior that a player uses to gain an advantage over his peer player(s) or achieve a target in an online game is cheating if, according to the game rules or at the discretion of the game operator (that is, the game service provider, who is not necessarily the developer of the game), the advantage or the target is one that the player is not supposed to have achieved.' I do not have a problem with putting terms like *hacks*, *exploits* and *cheats* in the same category and define them as *cheats*, because they often mean the same thing or at least have an overlap that makes them difficult to distinguish from each other, at least in the context of online gaming security issues. I do however want to take *attacks* out of this category, as I feel that some issues other authors refer to as cheats go beyond simply cheating, at least in the definition that accompanies the listing of these issues [7]. This leads to the distinction shown in the picture below:



I will further explain this distinction between attacks and cheats in section 3.1. After that, in section 3.2 I will describe and compare some frameworks used to classify different forms of online cheating, and pick one to work with in this chapter. Section 3.3 then describes the various issues I define as cheats. I will take the short definition offered by Yan and Randell [7], and try to improve, extend and clarify this definition where needed, as well as add some examples, mainly as found in MMO(RPG) games. In section 3.4 I will do the same, but then with the issues I define as attacks. Because many issues can be executed both as a cheat and as an attack, I have dedicated section 3.5 to these multi-purpose issues.

3.1 Attacks versus Cheats

In this section, I am going to make the distinction between attacks and cheats and try to offer accurate definitions for them. The main difference between these 2 categories is cheats being used *in*-game, and attacks being used *at* the game, or at the game's players.

The first thing to do is to create clear definitions, starting off with one for cheating. There is not one definition that is generally accepted because different game companies vary in the criteria used to determine which behaviors are cheating behaviors. The reasons for this [6] are:

- Online game cheating is a topic in its infantry to researchers;
- Wide variety of online game genres leads to different forms of cheating;
- Newer cheats are constantly invented as security companies defended the older cheats

The key in most cheating definitions is the same however: the gain of an *unfair advantage* over other players. With this I can make a definition for cheating, which is basically the same as the one I gave in the introduction of this chapter, with the exception that the authors [7] use this definition for both cheats and attacks, because this distinction is missing in their paper:

> Any behavior that a player uses to:
>
> gain an advantage over his peer player(s); or
>
> achieve a target in an online game;
>
> is cheating if, according to the game rules or at the discretion of the game operator (that is, the game service provider, who is not necessarily the developer of the game), the advantage or the target is one that the player is not supposed to have achieved.

Next up is the definition of attacks in an online gaming context. Although the above definition seems formulated very well, the authors also put the more serious attacks on the security of an online game, such as social engineering and compromising game servers under this definition. I think some of their 'cheats' exceed the definition they offer; because the actions performed have little to do with the gain of an unfair advantage. Also, where cheats are mainly in-game actions, attacks are mostly performed outside the game. A third difference between attacks and cheats is in their goal. The goal of an attack is often causing harm, or making money. The goal of a cheat is gaining an in-game advantage over (a) peer player(s). So the definition I want to use here for attacks here is:

> Any action that any person uses with the purpose of causing harm or gain economic benefit by:
>
> stealing a player's game account; or
>
> stealing other personal information of a player; or
>
> damaging, disrupting or compromising a game server;
>
> is called an attack.

A reason that other authors do not distinguish between attacks and cheats could be that this difference in practice is not always directly clear. Cheating does not start where attacks end, and vice versa. Moreover there are sometimes links between the issues. A cheat can lead to another cheat or an attack, and an attack can lead to another attack or a cheat. Sometimes, a cheat is not even a cheat, at least not in the view of a game operator, but simply *clever use of game mechanics*. For some of the issues goes that they can be executed both as a cheat and as an attack, as I will show later on.

3.2 Online Cheating Frameworks

There have been a few efforts to create a framework for online cheating. One of the most commonly cited ones was offered by Matthew Pritchard [5] and consists of six categories: *reflex augmentation*, *authoritative clients*, *information exposure*, *compromised servers*, *bugs and design loopholes* and *environmental weaknesses*. A criticism of this framework is that it is "ad-hoc" [6], and only covers a subset of the cheating behaviors that can be found in online gaming systems.

Another framework that was developed with the knowledge of Pritchard's framework consists of 11 categories [8] and was later revised to contain 15 categories [7]. For a quick comparison between the three frameworks:

Pritchard [5]	**Yan & Choi** [8]	**Yan & Randell** [7]
Reflex augmentation *Computer program replaces human reaction to produce superior results*	Cheating by modifying game software or data	Cheating by exploiting misplaced trust Cheating by exploiting machine intelligence
Exploiting authorative clients *A player's modified copy of an online game tells all the other players that a definitive game event has occurred*	Cheating due to lack of secrecy	Cheating due to lack of secrecy Timing cheating
Information exposure *On a compromised client, the player is given access or visibility to hidden information*	Cheating by collusion Cheating due to lack of secrecy Cheating by modifying game software or data	Cheating by collusion Cheating due to lack of secrecy Cheating by exploiting misplaced trust Cheating by modifying client infrastructure
Compromised servers *Some client-server games can be customized by the user running the server*	Cheating by modifying game software or data	Cheating by compromising game servers
Bugs and design loopholes *Any bug that enables cheating*	Cheating by abusing procedure or policy Cheating by abusing bugs or design flaws	Cheating by abusing the game procedure (renamed) Cheating by a bug or loophole (revised)
Environmental weaknesses *Causing extreme lag in network communications, to the point of a momentary disconnection to place multiple command requests in the queue*	Cheating by denying service to peer players	Cheating by denying service to peer players
	Cheating related to virtual assets	Cheating related to virtual assets
	Cheating by compromising passwords	Cheating by compromising passwords
	Cheating due to lack of authentication	Cheating by exploiting lack of authentication
	Cheating related to internal misuse	Cheating related to internal misuse
	Cheating by social engineering	Cheating by social engineering

As you can see, all of Pritchard's categories are covered by the other two, and an additional five categories are added by Yan and Randell. It must be noted that Pritchard used a very different approach than Yan and Choi and later Yan and Randell did. Therefore this table is only an

approach of how the categories in the framework compare to each other, not an exact mapping. Some definitions only partially match each other; the table simply shows where this match between definitions is the closest. The framework by Yan and Randell is simply a revision of the one provided by Yan and Choi. The categories listed in this framework are mutually exclusive; every cheat fits in exactly one of the categories. For the purpose of this thesis – describing and classifying cheats and attacks and testing them against existing countermeasures – I will adopt the 15 category framework [7], in which I will make some modifications of my own to improve the framework.

3.3 Cheating

Cheating in computer games has been around pretty much as long as computer games themselves. In earlier days however, games weren't played over the internet. Players were either playing in single player mode, or multiplayer with the other players sitting in the same room or at least very close. Cheats were not much of an issue back then, as gamers would most times only fool themselves when using one. Gaming software developers often added cheats to their games as a feature, like the 'famous' cheat *iddqd*[9] ID Software added to their shooter DOOM, which provided a player god mode, making him invincible. Cheats as these are not much of an issue when a player uses it to cheat the system in a single player game, but when players go online and use them to cheat each other; it's easy to see how this can cause problems. Of course, simple command line cheats are not supposed to be present in online gaming environments, and if they are, using them is directly visible to a cheater's peer players as well. Other cheats are present however, with a general rule saying that if there is an opportunity for players to cheat and gain an unfair advantage over their peer players, they will use it.

3.3.1 Forms of cheating

In this section, I will present the security issues from the framework [7] that I define exclusively as cheats. I will use the relatively short definitions Yan and Randell offer where needed, and adapt these definitions when I feel it is appropriate. I will add information where I think it is needed, and offer some examples of how these cheats come to play in an MMO environment.

3.3.1a Exploiting misplaced trust

The trust being exploited in this cheat is the trust a game developer puts into the game client. In reality, this security cannot be trusted at all; cheaters have total control over their game clients. Game code and configuration data can be tampered with on the client side. A cheater can try to play the game with a modified client program, or replace code and data on the fly, for example to access sensitive game states that are otherwise unavailable to players. [7]

The reason that the client software contains so much important code and data is that online games are often way too big to be fully controlled by the game servers. The servers only handles interactions, while the client software contains all the objects, textures, etc. that make the interactions with the server visible to the players.

A relatively innocent (and therefore mostly condoned) way of modifying the game client is changing a skin of a virtual character. Especially in role-playing games (in this case MMORPG's)

[9] http://www.urbandictionary.com/define.php?term=iddqd

such as World of Warcraft, you can make a small change to some texture files, for example to make your orc look like a troll, once you get bored of playing as an orc.
The additional service 'paid race/sex change' that Blizzard introduced in October of 2009 to World of Warcraft ended much of these practices. Players appeared to be more willing to pay a small fee to change their character's appearance than to mess around with game files, knowing it was not entirely in line with the game's policy.

A more serious case of modifying game client files became known in November of 2006. Players of the guild 'Overrated', one of the very best guilds on the US servers of World of Warcraft at that time, applied a file called 'patch5.mpq' to their clients. With this patch, they were able to completely remove a wall/floor in one of the 40 player dungeons, giving a whole new meaning to the term *wall hack*[10]. By doing so they were able to save many hours of fighting boring and unrewarding enemies, progressing directly to the more rewarding encounters. After several threads on the community forums, Blizzard struck down hard on the guild, permanently banning every player involved in the cheating. In a reaction, a player explained that they knew they had it coming, but that it was very much worth it[11].

3.3.1B Collusion

Many cheats in this category are found in online card games, such as bridge [9], where players can collude to get more information about the cards in the play than they should have, and thus gain unfair advantages over their honest opponents [7]. However, I want to focus on two types of collusion that are found in MMO games and other competitive e-sports.

The first type is the so called 'win trading'. Competitive games often have ladder systems, and players or teams of players battle each other to gain rating and progress on the ladder. To cheat on this, players or teams can simply agree to take turns in winning, to both progress on the ladder in a faster pace than honest other players. To make sure they would meet each other, they would play at times when few other players were active. This was particularly popular in the game Starcraft 1. A simple fix for this is to make a team that loses also lose rating points, and thus drop on the ladder, and designing it so that you gain the most ladder points by defeating a team with a rating close to yours. In the World of Warcraft arena system, players still got around this by constantly creating new teams to reset the rating of the lower ranked team, effectively working up teams one by one. A significant amount of bans followed a new fix that linked ratings not only to teams, but also to players, eventually fixed the cheat in World of Warcraft.

The second type of collusion is to my knowledge specific to World of Warcraft, because no other games use the mechanic that facilitates it. It involves the vote-kick tool used in the group-generation system used for 5 player dungeons. The tool was implemented to help players to progress through dungeons faster, by giving them the possibility to vote out players that are not cooperating, insufficiently contributing or misbehaving. The problem with this system is that it is automated and goes by a majority vote. Because players have the opportunity to join the queue for the group-generation system in groups of 3 or 4, they basically have full control over the other players that are picked to complete the group. This leads to players being removed for the wrong reasons, such as a request to communicate in English, making innocent mistakes, or being after the same items someone else in the group wants.

[10] http://wow.joystiq.com/2006/11/02/fighting-trash-mobs-is-totally-overrated/
[11] http://wow.joystiq.com/2006/11/06/overrated-responds-to-their-permaban/

3.3.1c Abusing game procedures

Like collusion, this kind of cheat is mostly found in competitive online games. Cheaters do not require any technical sophistication to carry out this cheat because they simply abuse the game's operating procedure. A common case of abusing game procedures in many online games is escaping: a cheater disconnects himself from the game system when he is about to lose. [7] Once again, the ladder system is involved, including the fix where a losing player or team loses rating. The logic that is being followed in the case of escaping is that you cannot lose rating if you do not actually lose the game, leading players to simply pull the plug or crash their game when a loss is unavoidable. An issue such as this is well known, and is therefore most likely already fixed before a game even gets released. The most common fix is to make a team or player lose rating if he does not finish the game within a certain timeframe. This timeframe is often quite short, but can sometimes be longer to give players who drop their connection unintentionally the opportunity to return and finish the game.

Many other cases of this cheat are quite innocent, and game developers often use the term *creative use of game mechanics*. The flaws in the game procedures are (hot)fixed as soon as possible, but cheating players are not punished for abusing them.

3.3.1d Exploiting machine intelligence

When a game can be modeled as a computable problem, cheater can sometimes exploit artificial intelligence (AI) techniques. If the maturity of AI research into such games is advanced enough, machine intelligence can have superiority over a human player. This can occur in many online games such as online chess and online versions of traditional board and card games. [7]

The definition of this cheat talks about programs running parallel to the game program to help a human player with complex computations to produce superior results. Other programs that fall under this definition are those that automate game play, having characters in-game move without the player actually being at his keyboard. This can be limited to simply taking a small step every minute, for example to prevent the character from obtaining the 'away-status'. In World of Warcraft, this is sometimes used by players in battlegrounds (advanced player versus player zones). When a player's character isn't controlled for 5 minutes, he automatically gets the away-status, removing him from the battleground. Having a program running that makes a move once in a while prevents this and lets the player get a lot of points without actually playing the game. Other examples are aim-bots in shooter games, which help a cheater hit the enemy player.

A special case of game play-enhancing programs are the so called add-ons or mods. These are usually not against the game policy, and their main purpose is to modify the in-game user interface. To make sure that they are not used for the wrong purposes, the syntax of the programming language of such add-ons is often limited so that no automated actions can be executed.

3.3.1E Modifying client-side system infrastructure

'Players can cheat by modifying the client infrastructure, such as device drivers in their operating systems.' [7] A graphics card driver can be modified to make a wall transparent so that cheaters can see through it, locating other players who are supposed to be hidden behind it. This is the so called wall hack, a popular cheat in online shooter games.

3.3.1F Exploiting a bug or loophole

This category sounds as a very generic category that could basically contain every cheat this chapter discusses. Yan and Randell [7] recognized this problem in the earlier version of the framework [8] they use, and thus revised the definition of the cheat.

'[C]heaters exploit a defect in game programs or the game design itself without having to modify game code or data. Once discovered, such a defect will give knowledgeable players a major advantage.' [7] In some ways, this cheat is similar to abusing game procedures, but in this case not the procedures are abused, but more general game mechanics are abused to gain an advantage. The most well-known example of this is when players get really creative in accessing areas in the game world that are supposed to be off-limits until they are officially released. Websites such as www.mmowned.com are places where a lot of information about this but also other types of cheats can be found.

3.3.1G Internal misuse

Game operators usually have system administrator privileges that can easily be abused by insiders; the game operator employees. They can generate super characters and valuable virtual items by modifying the game database on the server side. [7] Game operator employees (called game masters in World of Warcraft) exist to personally assist players when they have a problem inside the game, such as being stuck or being harassed by other players. They do for example have powers to move players to any location in the game world they want, and to create any item they want. It's easy to imagine how these powers can be abused for financial gain or just for fun.

A special case of this cheat is slightly different from the description above, and rarely occurs. This is when a game operator employee makes a mistake by providing a player by an item he shouldn't have gotten, and the player starts abusing the item while being fully aware that he shouldn't. In World of Warcraft, a player once received an item that gave him the ability to destroy any hostile unity coming near him, and promptly started killing his way through the latest 25-player content.[12] The end result was that the player in question got his account permanently banned from the game. This cheat itself falls under the category of 'abusing game procedures', but the cause of it was an internal mistake by an employee, and thus internal misuse.

Another special case is when internal misuse is combined with collusion, where a game operator employee and a dishonest player work together to achieve an unfair advantage for the player. Game operator employees often anonymously (to their peer players) play the same game outside their job, opening options for this kind of misuse, but risking both their job and their gaming account is not something they would easily do.

[12] http://wow.joystiq.com/2009/04/29/player-receives-developer-item-in-the-mail-one-shots-ulduar/

3.4 Attacks

As I stated before, I feel that some issues go beyond cheating, and therefore should not be defined as such. These attacks, as I have labeled them, do not give the offender an unfair in-game advantage over his peer player(s), but mostly work outside the game and serve to cause harm and steal accounts.

Yan and Randell [7] have a category labeled *compromising passwords*, which is then linked to a very generic definition of how passwords are being compromised. Next to that, they also offer several other categories that describe the various ways of how passwords can be compromised. This is a bit sloppy, as it suggests that there are more cheats (in their definition) or attacks (in our definition) than there actually are. The attack here is called *compromising accounts*, the categories Yan and Randell label as separate categories are in my view simply subcategories of this attack, and thus I will present them as such. Because many of the security issues that can be executed as an attack can also be executed as a cheat and my modifications to the *compromising passwords* attack, only one issue remains exclusively as an attack. This section presents this attack.

3.4a Compromising accounts

Key to pretty much all the data and authorization players have in an online game system are their passwords. By compromising such a password, an attacker can access the victim's game account, and use it for his own purposes or that of a middle market company, to steal the player's virtual possessions, or to spam and scam, indirectly damaging the reputation of the player.

Dictionary and brute force attacks

Players often choose a password that is easy to remember, but because of that, the password becomes easy to guess to an attacker as well. Brute force attacks are another way to get access to accounts if the target authentication system does not adequately protect against this.

Malicious software

When a game's popularity increases, the amount of game-related websites and fan sites grows accordingly. The more of such websites rise, the bigger the chance some of them are set up with less noble intentions. The average gamer – especially when a game is as accessible as modern MMOs are – is not a very experienced internet user, and it generally takes little effort to fill a computer with various toolbars, Trojan horses and key loggers. When someone visits a website related to World of Warcraft, there's a good chance he actually owns a World of Warcraft account. More popular fan sites attract thousands of visitors each day, and often include ads to compensate for their expenses. These ads can sometimes contain malicious code as well, as attackers are aware of how many people actually visit such websites without any decent protection against scripts.

Social engineering

Tricking honest players into handing over their ID and password by making them believe something attractive or annoying has happened to them is another way for attackers to get a hold of players' accounts.

This is an issue that is not exclusive to online gaming; online banking deals with the same problems. It is however one of the biggest issues to MMOs, for reasons I have already discussed in section 2.4.
There are several popular ways for attackers to attempt to get honest players to provide them

with their login details. Players are either contacted through email or in-game chat or mail. The attacker attempts to make a player (generally hundreds at once) believe he represents the game operator. Of course, a player does not simply provide his login details because he is asked to do so. So, as mentioned they attempt to trick players into believing that either something attractive or something annoying has happened to them.

Several examples of how this is executed in practice can be given:
A player is being told he has been awarded a rare in-game item, or that he has been selected to participate in an upcoming beta-test. A link to a website is provided where he should login to claim his reward. The login page of such a website often looks exactly like the one you find on the account management page of the game, apart from the URL of course.

Similarly, an attacker masking as a game operator tells a player that there is evidence of the player trying to sell his account, and points out that this is against the policy of the game. If the player does not verify his login details within a certain amount of time, his account will be closed.

In online gaming, a curious thing about these phishing attempts is the language used in these mails or messages. It's not just the URL's of the websites players are pointed to that are (often obviously) off, but also the message itself is more often than not infested with spelling- and grammatical errors.

Another thing that is alarming is the amount of topics that is being created on game-related forums, asking "is this mail legit?" Apparently, players have trouble identifying whether mails are from game operators or from attackers.

How do attackers get the email addresses of players? Once again the game-related websites I mentioned in chapter 3.3a come to play. Many of these websites contain forums, and thus require registering. All this data ends up in a database, yet another prey for an attacker. This becomes even more interesting when you consider the fact that many people do not add a lot of diversity to the passwords they use on different systems.

Exploiting lack of authentication

Attackers can attempt to collect many ID-password pairs from legitimate players by setting up a bogus game server, if there is no proper mechanism in place for authenticating a game server to a client. When there is no proper mechanism for authenticating a client, this can be exploited by attackers as well. [7] When a player prompts the system for a password change, it is important that the system re-authenticates the player to make sure it's the actual account owner requesting the change, and not someone with temporary access to the account. Internet-cafes are places where such attacks often occur, especially in Asia where the majority of the gamers play from internet-cafes.

Exploiting lack of secrecy

When game clients send players' passwords to the server in plaintext format, eavesdropping can lead to these passwords being compromised.

3.5 Multi-purpose issues

Now that I have made the distinction between cheats and attacks, it becomes apparent that some of the security issues aren't exclusively a cheat or an attack; they can be executed either as a cheat or as an attack. One way to deal with this is list them under both categories, but for the

purpose of overview I have decided that making a new category for this is a better option.

3.5A Compromising game servers

Attackers can tamper with game server programs or change their configurations once they've obtain access to the game host systems. [7]
Earlier I have pointed out that because of a game being reliant on a connection to a game server to function at all, the biggest security issue of games - and other entertainment such as music, movies and literature - , namely piracy, is no longer much of an issue at all. This however is not entirely true. Once someone gets himself access to the server software of a game, he can copy (or emulate) it and start his own game server. With this he is effectively committing piracy and thus breaching copyright. The term used for such a server is 'private server'.

Above definition for this issue as provided by Yan and Randell [7] made me classify it as an attack. However, the definition offered by Matthew Pritchard shows that it can also be explained as a cheat, in which there is a gain of an unfair advantage, but no real harm is being caused. Some client-server games can be customized by the user running the server:
'Access and configurability are great for many games, as they allow the player community to extend and evolve a game. But some individuals will test the server to see what can be exploited in the name of cheating. This in itself is not the problem - rather it's when honest but unaware players find their way to the server and do not know that they are not on a level playing field.' [5]
In both compromising servers as a cheat and compromising servers as an attack the game servers are ran by people other than the game operator. The difference here is that the in the 'cheat-version' players are tricked into playing on servers that has been tampered with.

3.5B Exploiting lack of secrecy

Already mentioned as a subcategory of compromising passwords, eavesdropping can also be used to insert, delete, or modify game events or commands that are transmitted over the network in plaintext or using a very weak encryption. Obviously, this cheat realistically should not be able to occur in a big game like World of Warcraft because of the size of this game and the impact this cheat would have on it, but it is still something for game developers to take into account when designing a new online game.

3.5C Denying service to peer players

By denying service to peer players, a dishonest player can gain advantages over them. Cheaters can delay responses from their opponents by flooding the opponents' network connection. Other peer players would then be cheated into believing that something was wrong with the victim's network connection and agree to kick the player out of the game to avoid him stalling the session. [7] Denying service to a single player is a cheat, doing so for an entire server is classified as an attack.

An interesting case of a denial of service (DoS) attack is discussed by Bono et al. In pretty much every MMO, there is a command line interface. For regular players, the main purpose of this command line interface is to communicate with each other similar to the way they do in chat rooms and instant messaging programs. However, this command line interface can also be used to execute various commands. In the discussed 'Buffer Overflow: Crash Example' [10] an exploit

causing a crash in a peer player's game client in the MMORPG Anarchy Online is described. Because the game has very few limitations on the commands that can be issued, an attacker is able to execute files anywhere on his peer's computer. 'If a script is loaded with a single line that's longer than 1,024 bytes, a stack buffer overflows, the executable in memory becomes corrupted, and the game client crashes.' The exploiter can thus simply let his peer player's client execute a large file, such as the 18 Mb game client executable, and crash his game client.

A special type of a DoS attack is a distributed denial of service (DDoS) attack. Here the goal of the cheater is not to deny service to a single peer player, but rather to anyone using a specific server. This is not something that happens on a regular basis, but sometimes it does happen. Early in 2010, one European World of Warcraft server was being disconnected quite a lot, and the story went that a single player was behind this, abusing an in-game macro to overload the server. Angry players went on a witch-hunt and tracked down the Facebook profile and other personal information of the assumed attacker. Blizzard eventually resolved the issue, but never made an official statement about what had been going on.

3.5D Cheating related to virtual assets

Especially in MMORPGs, virtual assets play a big role. Players can trade virtual items and currency with each other, similar to how a real-world market works. Additionally, these trades can exist between virtual property such as in-game items and currency (but also virtual characters or even entire accounts), and real money. The issue that immediately rises here is scamming. A player delivers as promised but never sees a payment, or vice versa. I distinguish three categories here: in-game scamming, scamming or otherwise cheating between game and real world (dealing in virtual items or currency with real money) and scamming or related issues outside the game (dealing in accounts). It is a bit tricky here to draw the line between cheating and attacking, I decided to classify in-game scamming as a cheat and scamming or related issues outside the game as an attack. The last category is realistically closer to cheating as well, as there is still an unfair advantage to be gained, but may very quickly lead to the offender becoming the victim as he starts doing business with shady middle-market companies.

Different games have different rules. Whereas in Second Life transactions between virtual and real world money are more or less a feature of the game, in World of Warcraft it is absolutely not allowed. Selling a character or an account is, when discovered, something that gets the account in question permanently banned from the game, making it useless to anyone (this directly leads to one of the social engineering methods discussed earlier). Any World of Warcraft account is ultimately still the property of the game operator, and although a player gains some rights by creating an account and subscribing to the game, making real money on it is not one of those rights.

Common in-game cheats that relate to virtual assets are in-game scamming and ninja-looting. To prevent scamming in World of Warcraft, some small features are in place. The trading interface works in a way that when one player accepts the trade, the other can no longer modify the items or currency involved in the trade. 'Gift wrapped' items cannot be sent through the mail-system, as the receiver is unable to see the contents of the item he is paying for. To reduce the impact for players who still get scammed, they usually get all their items returned to them, while the offender can expect a (temporary) ban. Items from the trading card game (a real world

collectible card game[13]) also offered a lot of opportunity for scammers. Some of these cards offer loot codes for very rare in-game items, which led to fake loot codes being sold for a lot of in-game currency. To fix this, the reward items themselves where changed so that they could be traded directly. Tricking players into buying auctions with extremely high prices is another way of in-game scamming; avoiding this generally comes down to the intelligence of the players themselves.
Ninja-looting can occur when a group of players puts their trust into one player to handle the items that drop on an encounter. This player is then the only one able to assign items to their rightful owners, and can decide to simply take everything for himself or his friends.

Other cheats are related to middle-market companies I talked about in chapter 2. Players can spend real money to obtain power leveling services or in-game currency. Doing so gives them an unfair advantage over other players, and can upset the in-game economy so game policy documents often explicitly forbid this.

Real world dealing in virtual assets can sometimes be very tricky and hard to prove. Because of this, the auction website eBay decided early 2007 that they would no longer support auctions of virtual goods from online games, with the exception of Second Life.[14] There are however many more websites that facilitate virtual property trading and many of those are linked to shady middle-market companies that are also involved in botting, gold-selling, in-game spamming and compromising passwords. A conclusion to be drawn from this is that selling and buying virtual property is not only in most cases against a game's policy, but also very risky.

3.5E Timing cheating

In massively distributed systems, time and state are very important. Because so many players interact through their client software with the server simultaneously, many types of race conditions can occur. Sometimes, cheating players can delay their own moves until they know all of their opponent's moves, and thus gain a huge advantage. [7] Baughman and Levine [11] describe several complex timing cheats in both client-server and distributed architectures.

An example of a timing cheat that exists in MMORPGs, but is far from exclusive to them or even to games, is 'sniping' auctions. One of the features MMORPGs are known for are auction houses to buy and sell in-game items. A player can either bid on an item, or directly buy it for a fixed, amount set by the seller. Now someone can try to bid on such an item right before the auction expires, effectively *sniping* it away from the player who thought he was going to win it.
Of course this is in no way exclusive to online games, as the internet is filled with tons of online auction websites where people can effectively do the same thing. A simple fix that deals with this issue in World of Warcraft is to simply increase the time left on an auction by five minutes every time a new highest bid is placed.

An interesting attack that involves timing is described by Hoglund and McGraw [1], where you can in theory play a subscription game for free by cancelling your account after every session, because a session is usually shorter than the time it takes for the game operator to bill you. Of course, cancelling and reactivating a game account several times per day or week eventually draws attention, and a proper mechanism should completely remove the possibility for this attack to take place at all.

[13] http://en.wikipedia.org/wiki/World_of_Warcraft_Trading_Card_Game
[14] http://news.cnet.com/eBay-bans-auctions-of-virtual-goods/2100-1043_3-6154372.html

4 Security Analysis of the Issues

In this chapter I am going to analyze various security features of the issues I have discussed in chapter 3. First I am going to introduce and explain the features that will be looked at, and after that a table will show how the issues score on these features. I included the subcategories of *compromising accounts* in the table because however similar they are, some small differences still do exist, making it less optional to only analyze *compromising accounts* as a whole. It must be noted that the high/medium/low rankings in the table are for the major part based on my own knowledge and observations. Below are the features that I am going to look at:

- **Exclusive to gaming**
  Many issues are not exclusive to gaming, especially when you look at something like *compromising accounts*, this is an issue pretty much any system that contains user accounts has to deal with. The issues I checked as *exclusive to gaming* are not exclusive to gaming per se, but I believe the likelihood they are found in systems not related to gaming is not significant.

- **Relevance to MMOs and Relevance to other games**
  Earlier I have explained why MMOs are the most relevant type of online game when looking at security issues. These two columns show why. The reason why MMOs are only partially relevant to *collusion* and *abusing game procedures* is that they are very specific to direct player-versus-player competitive games. Even though some MMOs do contain such player versus player elements, they are not the major aspect of such games.
  In other games (as defined in section 2.2), that have a mainly competitive aspect, these player-versus-player elements are the major elements of the game, and thus they do have a high relevance to such cheats. Because these games generally fall into the *charge for software license* category from section 2.2 and because the accounts involved don't increase in value over time as no virtual property is accumulated, the threat of *compromised accounts* is relatively small.

- **Offender**
  This column shows the main offender of the cheat or attack. An offender can either be a player of the game, an insider (a game operator employee), or an outsider.

- **Victim**
  This column shows the main victim of the cheat or attack. The victim can be a player or the game operator.

- **Vulnerability**
  Here, the vulnerability being exploited is shown. Once again, the vulnerability can be a player, or the vulnerability can be found at the side of the game. The different vulnerabilities at the side of the game are the *game client software* which can be insecure, or be tampered with; the *game operator* which can be misled; the *game mechanics* including both the design and the implementation, which can be flawed; and the *game system* as a whole, consisting of the game servers, the authentication servers and the network, which can be insufficiently secured against some issues.

- **IMPACT**
  This column shows the impact each cheat or attack can have on their victim.

- **PROBABILITY**
  In this column it is shown how big the probability is that a cheat or an attack occurs. For the issues that have a medium or low probability, often the most standard security measures already deal with them (such as making sure information is always being encrypted before transferring), simple fixes in the game code make them very unlikely to happen, or there are incentives in place that make sure an issue is not very likely to happen (such as losing a job for internal misuse).

- **PUNISHABLE BY LAW**
  This one can be a bit tricky. It show which attacks (as cheats are defined within the game and thus generally have no consequences outside the game) could lead to lawsuits. This does not mean that a lawsuit against the offender of such an attack is guaranteed to be successful, or that it is even sensible to start such a lawsuit. Evidence and liability are often difficult to find and prove, and the impact of such a case is normally way bigger than the impact of the crime committed. This is probably best illustrated in the *cheating related to virtual assets*-attack, where eBay does not want anything to do with disputes over virtual property (see section 3.5d).

  In the table, I indicate that four categories of attacks that are, or could be, punishable by law. These four categories are:
  - *Compromising accounts*
    Some of the attacks that lead to compromised accounts are very similar to those used in online identity theft. Countries all over the world already have or are working on legislation to deal with these types of cybercrime, greatly supported by the Council of Europe's Convention on Cybercrime. In December 2009, China sent eleven people to jail time for being part of a gang that created malicious software and used it to compromise online gaming account details[15].
  - *Compromising game servers*
    Gaining access to server software to copy and emulate it (as I have defined as a *compromising game servers*-issue) has been found illegal in the case of Blizzard vs. BnetD[16] because it was in violation with the DMCA and Blizzard's EULA (see section 5.1).
  - *Denying service to peer players (distributed denial of service)*
    DDoS attacks fall under tort law, and are generally reason to start a lawsuit against the offender [12]. However, because the rarity of such attacks within online games and the various liability issues that can rise, a game operator is likely to deal with the problem on its own, especially when the attacker is a player of the game.
  - *'Cheating' related to virtual assets*
    This last category is one that is currently in full development when it comes to ownership rights in the creation and use of virtual property, as is discussed in an article by Woodrow Barfield [13]. Several court cases have occurred between game software companies (Worlds.com vs. NCsoft[17]), between gamers and game software companies

[15] http://www.theregister.co.uk/2009/12/17/china_jails_game_trojan_vxers/
[16] http://www.eff.org/cases/blizzard-v-bnetd
[17] http://massively.joystiq.com/2010/04/27/worlds-com-vs-ncsoft-lawsuit-settled/

(Bragg vs. Linden Research (developer of Second Life)[18], and Second Life "residents" vs. Linden Lab[19]) and between gamers (Eros, LLC vs. Simon[20]) dealing with various disputes over virtual property in online games.

As you see, several laws are used to attempt to deal with security issues in online games. It is however a field that is in full development. One problem here is the difference in law or implementation of law between countries. The DMCA is a United States copyright law; Europe has the European Union Copyright Directive (EUCD) which addresses some of the same issues as the DMCA. The Council of Europe's Convention on Cybercrime has been ratified by many countries outside Europe, including the United States. Because of the developing field of cyberspace law, and mainly those laws on copyright and virtual property, many issues are dealt with on a case-by-case basis, as you can see in the cases I mention under *cheating related to virtual assets* above.

4.1 TABLE

After describing the columns used in the table, it is time to show the table itself. In the table all the issues discussed in chapter 3 are scored on the features above.

[18] http://en.wikipedia.org/wiki/Bragg_v._Linden_Lab
[19] http://articles.latimes.com/2010/apr/30/business/la-fi-lazarus-20100430
[20] http://www.citmedialaw.org/threats/eros-llc-v-simon

Issue \ Feature	Cheat	Attack	Exclusive to gaming	Relevance to MMOs	Relevance to other games	Offender	Victim	Vulnerability	Impact	Probability	Punishable by law
Exploiting misplaced trust	✓			High	High	Player	Player / Game operator	Game client	Medium	Medium	
Collusion	✓		✓	Medium	High	Player	Player	Game mechanics	High	High	
Abusing game procedures	✓		✓	Medium	High	Player	Player	Game mechanics	High	High	
Exploiting machine intelligence	✓		✓	Medium	Medium	Player	Player	Game mechanics	High	High	
Modifying client infrastructure	✓		✓	Medium	High	Player	Player	Game client	Medium	Medium	
Exploiting a bug or loophole	✓			High	Medium	Player	Game operator	Game mechanics	Low	High	
Internal misuse	✓			High	Low	Insider / Player	Game operator	Game operator	High	Low	
Compromising accounts		✓		High	Low	Outsider	Player	-	High	High	✓
Dictionary and brute force attacks		✓		High	Low	Outsider	Player	Player / Game system	High	Medium	
Malicious software		✓		High	Low	Outsider	Player	Player	High	High	✓
Social engineering		✓		High	Low	Player / Outsider	Player	Player	High	High	✓
Exploiting lack of authentication		✓		High	Low	Player / Outsider	Player	Game system	High	Medium	
Exploiting lack of secrecy		✓		High	Low	Outsider	Player	Game system	High	Medium	
Compromising game servers	✓			High	High	Player	Player	Game system	Medium	High	
		✓		High	High	Player / Outsider	Game operator	Game operator	Medium	High	✓
Exploiting lack of secrecy	✓			High	Medium	Player	Player	Game system	High	Medium	
Denying service to peer players	✓			High	High	Player	Player	Game system / Player	High	Low	
		✓		High	Medium	Player	Player / Game operator	Game system	High	Low	✓
Cheating related to virtual assets	✓		✓	High	Low	Player / Outsider	Player	Player	Medium	High	
		✓		High	Low	Outsider	Player	Player	High	High	✓
Timing cheating	✓		✓	High	Medium	Player	Player	Game mechanics	Medium	High	
		✓	✓	High	High	Player	Game operator	Game operator	High	Low	

5 Protection Methods

In this chapter the various measures that are currently taken by game operators and gaming software companies to combat the security issues are discussed. Distributors of online games and those of MMOs in particular, have two weapons they can use against cheaters. The first one is making rules with legal documents, while the second one enforces rules with technology [1]. Section 5.1 deals with the first one, while sections 5.3, 5.4 and 5.6 deal with the second one. Sections 5.2 and 5.5 then explains what protection can be used against attackers, and finally section 5.7 tells about how players which have fallen victim to (mainly) attackers are being supported.

5.1 Legal documents and license agreements

First of all, there is copyright law such as the Copyright Act, title 17 of the US Code, and similar copyright laws that are in place or are being developed in countries all over the world. These laws talk about the rights and the limitations to the rights of copyright holders and the conception of *fair use*. Then there is the DMCA (Digital Millennium Copyright Act) in the United States, which criminalizes both the production and distribution of technology meant to circumvent copyright surrounding security technologies that are meant to enforce copyright laws. Although piracy, and thus copyright is not as big an issue in online games (especially the ones with a paid subscription model, such as groups 2 and 3 in section 2.2), there are still some cases where these laws are relevant, such as the case of emulation I discussed in section 3.5a, but also completely different issues[21].

In pretty much every software application you install these days, and thus also in online games, legal documents are included. These documents are the EULA (End User License Agreement) and the Terms of Use (ToU, sometimes Terms of Service (ToS) or Terms of Conduct (ToC)). The EULA is a legal contract between the software producer or operator and the end user, stating how the software is supposed to be used. The ToU documents often accompany a EULA for any client-server game and restrict the uses of the game on the server side. They typically also include terms that forbid vaguely defined forms of behavior and communication, and provide the game operator with the right to terminate the license at any time if these license agreements are violated. [1]

The problem with these license agreements is that they can contain seemingly the weirdest restrictions and notions, as Hoglund and McGraw discuss [1]: a EULA can state that the software is allowed to install backdoor root kits on your system (Sony BMG[22])or gain full access to your memory (Blizzard, see section 5.3). It can tell you that when you agree to it, you will also agree to all future unwritten EULAs, may not publicly criticize the product, may never uninstall the software, or take full responsibility for the actions of the software. Once you sign a EULA however, contract law dictates that you have to follow it. This does not mean that you cannot challenge a EULA in court; if the contract terms are sufficiently objectionable, there is a chance they won't hold, as was the case with Sony BMG's backdoor root kits.

These license agreements are there on a take-it-or-leave-it basis; if you do not agree with them, that is fine, but you will never play the game. The majority of the players of a game never read the agreements they accept, they just take them as a hurdle to get to play the game, and thus are rarely aware of what is actually in them.

[21] https://www.eff.org/cases/marvel-v-ncsoft
[22] http://www.cigital.com/papers/download/0601sec.sony.pdf

5.2 Creating a stronger authentication

The first direct way of safeguarding the security of a game and its players is by creating a stronger authentication method, beyond the standard login/password or email/password. Replacing the standard authentication method (something you know) by biometric scans (something you are) does not seem to be a viable option now or in the near future, because of the costs that are involved to make remote use of such scans secure – biometric information scanned on client systems can still be intercepted and thus stolen. The technology does not seem to be quite there yet when it comes to securely implementation of such methods on a large scale.
However, increasing security by adding additional layers, by including simple devices (something you have) is very much possible. In this section, I will describe 2 of such methods, both currently being used by Blizzard Entertainment.

5.2.1 Blizzard Authenticator

At June 28 of 2008, Blizzard Entertainment introduced the Blizzard Authenticator, meant as an additional security layer for users to protect themselves against account theft. The Blizzard Authenticator is currently used for the game World of Warcraft and the surrounding service Battle.net, but will also serve its cause for future (semi-) online games from Blizzard Entertainment. The authentication devices were being sold to gamers. About one year after the introduction of the authenticator, a mobile version was introduced, usable on iPods, and many modern mobile phones.

The authentication device works as follows: A player obtains (buys) a device (or downloads a mobile application) and links it to his gaming account (in this case the Battle.net account). Upon logging in to any service linked to this account, not only a username and a password, but also an authentication code is required. The device (or application) produces a user-specific 8 digit code every 15 seconds which remains valid to login with for about 2 minutes. When all login information is provided and correct, access to the account is granted. When either of the supplied login credentials is incorrect, login fails.

Gamers assumed absolute safety with an authenticator, but at the end of February 2010 the first cases of users having their account security breached even though it was linked to an authenticator became a fact. Attackers had found a way around the authenticators. They installed a file on a player's computer to help them execute a man-in-the-middle attack. The file did not only intercept the username and password, but also the authentication code. While doing so, players were tricked into believing the information they had entered was invalid as the file sent an invalid code through for authentication instead of the valid one. In the meanwhile, attackers could grant themselves access to the account in the small window the authentication code was still valid. If the player uses enough attempts to try and get into his account and thus provided the attackers with multiple authenticator codes, they could technically even login to the player's account management and replace the player's authentication device by their own. Some additional security measures to combat account theft are in place: a generated authentication code is only valid for logging in once, and to unlink and authenticator from an account, 2 consecutive authentication codes must be submitted.

5.2.2 Battle.net Dial-in Authenticator

In November of 2010, Blizzard released an additional free opt-in service to strengthen a player’s account security; the Battle.net Dial-in Authenticator. Unlike the Blizzard Authenticator, this does not involve a physical device or program, but it provides a service that actively monitors an account and requests additional authorization from the user when a potentially unauthorized login attempt occurs. If for example a player using this service is to login from a different location than from where he normally plays, he may be asked to call in and provide his personal PIN (chosen when enabling the service) to receive a unique, one-time use security code before access

to his account is granted.

Although Blizzard describes the dial-in authenticator as an extra layer of security, it is intended only for players who cannot afford or use a Blizzard Authenticator. Both additional layers of security are mutually exclusive, and while the dial-in authenticator can save players who always play from the same location from the hassle of having to enter an additional security code, it is less secure.

5.3 Detection and response

Aside from the Warden software discussed in 5.3, there are many ways of cheating that can't be detected simply by monitoring memory. Normally, game operator employees are there to detect these issues, either by directly spotting them, or by monitoring the game logs. When a game becomes as big as World of Warcraft however, with hundreds of servers worldwide and hundreds to many thousands of players on each of them, this method becomes simply impossible. Because of this, the game operator has to rely a lot on reports from players to track down offenders, which no longer strictly falls under detection. Some actions do of course still trigger some alarms in the game logs, such as when supposedly unavailable items get obtained by players. Reports from players are dealt with by game operator employees where needed using game logs and chat logs, and in line with the Terms of Use, temporary or permanent bans can be applied to the accounts of cheaters and attackers.

5.4 Monitoring players

This protection method is an extension to the previously mentioned *detection and response*, and I feel it deserves to have its own section in this chapter because it is significantly different from general detection methods. To prevent players from using software to automate game play in online games, they sometimes feel the need to go beyond the usual anti-cheat methods to stop players from using this software.

Although I did not identify the cheat *exploiting machine intelligence* as one potentially punishable by law, one case has occurred where Blizzard Entertainment sued and won against the creator of the 'botting'-software Glider[23], that automated game play in World of Warcraft through the use of scripting to perform repetitive tasks while the user is away from the computer. The court ruled that Glider was infringing the DMCA, and agreed with Blizzard that World of Warcraft is licensed, not sold. Blizzard also claimed the money that was earned by distributing Glider (approximately 100.000 copies were sold for $25 each), but was denied in this by the court of appeals[24]. Since May of 2009, World of Warcraft's EULA and Terms of Use forbid any third party to commercially exploit bots and other software related to the game.

The way Blizzard monitors users for using bots and other software that facilitates cheating is interesting. The program Warden was discovered in the fall of 2005 by self-taught computer hacker Greg Hoglund[25]. Warden is embedded in World of Warcraft, and actively monitors what is happening on a player's computer when playing. It monitors the World of Warcraft process space and keeps track of DDLs running in that space, checks around in other processes, reading text in the title-bar of every window and scans the code of every process that is running on the computer. [1] This clearly is an invasion of privacy, and has caused a lot of protest on forums and

[23] http://www.mmoglider.com/
[24] http://www.virtualworldlaw.com/Appelate%20decision.pdf
[25] http://rootkit.com/blog.php?newsid=358

elsewhere. Yet, accepting the EULA and Terms of Use means that you agree to be subjected to this type of monitoring.

Blizzard certainly is not the only company taking these kinds of measures to protect the security of their software. As long as these measures are included in the EULA and ToU, they are legally binding, unless successfully challenged in court, as was the case with Sony BMG's backdoor root kit software I mentioned in section 5.1. Maybe the Warden is not a big deal per se, and a company regarded as highly as Blizzard *probably* won't abuse the data it gathers. But if Blizzard is allowed to do this, what is the next step? And what stops other software companies from doing the same, until there is one that starts to abuse gathered data? It certainly is an interesting topic in the evolving field of cyberspace law.

5.5 Educating players (creating awareness)

Educating people to make them aware of security issues and intrusion methods is one of the easiest methods in attempting to prevent cybercrime, especially when it comes to identity theft [14]. It is an important topic in the financial sector (banks, credit card companies) and to governments.
Similar, educating players to make them aware of the issue of compromised accounts is a cheap and easy method to combat this issue, albeit not the most effective method. It is simply a matter of gathering information that is common knowledge to many game operator employees as well as players, and making it available to all players. The communities surrounding online games can play a big role in this, with players sharing information on forums and creating best-practices to deal with account security.
The game operator itself can contribute to this by highlighting valuable forum topics, but also by displaying security tips on login-screens and loading screens ("Tip of the day: A Blizzard employee will never ask you for your password").

5.6 Regular updates (patches)

One important feature of online games that most other games do not have, are the regular updates to these games, often in the form of patches. These patches bring new content to a game and update old content, but also fix bugs. Depending on the impact a bug has, the probability it is going to be abused on a large scale and the location where the fix has to be applied (server or client), a game operator can choose to repair a bug immediately (hotfix), wait for the next scheduled patch or server restart, or implement an additional patch for players to download and apply to their client software. Of course, when adding or updating content to a game, there is a big chance new bugs will slip in, or old code will break. Internal as well as public testing do their job to prevent this, but as with every software, the best testing is live-testing – that is, when games or patches are already released – and therefore some bugs will always slip through. Because of this, big content patches are often quickly followed by one or more hotfixes and small patches.

5.7 Victim support

When operating a subscription based online game, especially when that game is an MMO, customer support plays a big role in assisting players with their issues. When players get *hacked* (which is the faulty term players generally use when their account gets compromised) or

scammed, customer support should assist those players adequately to prevent them from walking away from the game completely.

In World of Warcraft, players who find out their account has been compromised are referred to the customer support section of the World of Warcraft website, where they can queue for assistance by providing their details. Account support can then lock the account to prevent any more abuse of the account during the investigation. Because of the size of the player base, and the frequency with which accounts are being compromised, restoring a compromised account can take days or even weeks. To somewhat ease the burden of this on customer support and to get players back in the game more quickly, Blizzard offers victims so called care-packages[26] [27] to directly close the investigation. These care-packages contain a predetermined compensation for the losses suffered from compromised accounts. Although this is not a very customer friendly way of dealing with the issue, it is ultimately the player himself who decides whether or not he accepts it.

When it comes to in-game scamming, players can often directly deal with game operator employees in the game to have their lost items or currency returned to them, and to have the scammer temporarily banned for his actions.

[26] http://wow.joystiq.com/2010/01/08/account-administration-told-not-to-restore-hacked-characters/

[27] http://wow.joystiq.com/2010/01/08/blizzard-policy-changes-in-reaction-to-account-security-concerns/

6 Review of Protection Methods

Just like security issues, protection methods can also be classified and be subjected to a security analysis. This chapter takes the protection methods from the previous chapter, scores them on several points and shows which of the security issues each of them deals with, or is supposed to deal with. With that information, problem areas can be indicated where issues (especially the high impact/high probability) are not adequately dealt with. After that, room for improvements in the dealing with these issues can be discussed.

The first table shows which security issues are generally targeted by which protection method:

	Cheats												**Attacks**				
	Exploiting misplaced trust	Collusion	Abusing game procedures	Exploiting machine intelligence	Modifying client infrastructure	Exploiting a bug or loophole	Internal misuse	Compromising game servers	Exploiting lack of secrecy	Denying service to peer players	Cheating related to virtual assets	Timing cheating	Compromising accounts	Compromising game servers	Denying service to peer players	Cheating related to virtual assets	Timing cheating
Legal documents	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓		
Stronger authentication													✓				
Detection and response		✓		✓	✓	✓	✓							✓		✓	✓
Monitoring players	✓			✓	✓					✓					✓		
Educating players											✓		✓			✓	
Regular updates		✓	✓	✓		✓			✓			✓					
Victim support											✓		✓				

As you can see, all cheats except one are covered by legal documents and at least one more protection method. Cheating on privately hosted game servers is something that in most cases falls outside the scope of the game operator and thus also outside the range of issues they protect themselves against.
Victim support, stronger authentication and educating players only cover very few issues, but these issues are the ones that request protection the most.

The next step is to score the protection methods on four features; effectiveness, cost, whether they create other issues in the process of attempting to solve security issues and what their weaknesses are. It must be noted that these scorings are largely based on my own experiences and estimations; numbers on effectiveness and costs are not readily available and requests to

gaming software companies to share these numbers are most likely to be ignored. Nevertheless I think I can sufficiently defend my comparison of the protection methods on these features. It can be argued if it is really viable to score protection methods in general, rather than per game or per game type.

- **EFFECTIVENESS**
  Where the above table shows what issues are combated by the protection methods, this column shows the overall effectiveness of the methods. The reason that some methods do not have a high effectiveness will be explained later, although some of them deserve some additional explanation:

  - *Legal documents*
    Legal documents have a medium to low effectiveness in general, simply because people aren't aware of what is in them. They are presented to players after installing a game, with a choice to decline them because game operators are obliged to do so. Few players actually take the time to read through them though. When it comes to attacks, the effectiveness of legal documents is low, attackers in most cases are aware of their actions being unlawful, they simply do not care;
  - *Stronger authentication*
    This is a very good way to improve the security of a game. However, the effectiveness of such a method is lowered slightly for two reasons: first off all, it should not be a mandatory method to every player, which means that the players most careless about their security are still very vulnerable. Second, when players think they are absolutely safe against anything that can compromise their game account, they might become more careless about the security of it overall, and neglect the importance of anti-virus software, firewalls and checking the source of URLs before opening them.

- **COST**
  This is somewhat tricky to determine, as I have already explained above. However, some estimates on the relative cost of protection methods can be made.
  - *Legal documents*
    The relative cost of legal documents is low, because some of these documents and laws are there regardless of the game (such as the DMCA), and other laws dictate that a game should contain these documents no matter what. However, once a security issue leads to a lawsuit, the costs do increase significantly. On the other hand, threatening to sue is for a game company sometimes enough to have possible offenders back off [1].
  - *Stronger authentication*
    For the two methods of stronger authentications I have described, most of the cost comes with the software that has to be developed to make them possible. In the case of the physical authentication token, letting players use the software on their own device (such as their mobile phone) is relatively cheap. Distributing actual devices costs more money, but this is somewhat mitigated because players pay for this. Returns to scale make it significantly cheaper for an online game with a large amount of players, and it certainly isn't something a lot of online game operators will be implementing (for now);
  - *Monitoring players*
    Once again, the biggest cost is in the development of the software, but that shouldn't be too high for a company already specialized in creating software;
  - *Educating players*
    One of the cheapest protection methods, because of the large role the community of an online game plays in it. The game operator simply has to guide and facilitate this process;

- *Detection and response*
  Employees have to be paid and trained to take care of this;
- *Regular updates*
  Expensive, but necessary to keep an online game running at all;
- *Victim support*
  Pretty expensive, because once again employees must be paid and trained for this, and many investigations that can consume a large amount of time have to be conducted.

- **CREATES OTHER ISSUES**
  Two methods create new issues in the process of solving security issues:

  - *Legal documents*
    Confusion is caused among some players when they get punished for violating the terms and agreements they accepted, because they are often not aware that their actions are not allowed within the game. This is only a minor issues however, and educating players can play a role in resolving a lot of this confusion;
  - *Monitoring players*
    As section 5.3 already discusses, directly monitoring the players' computers invades the privacy of these players, and it's questionable if invading the privacy of every single player is a fair trade-off for stopping players from using illegitimate software and add-ons.

- **WEAKNESS**
  Already partially explained under the header of effectiveness, this column should speak for itself.

	Effectiveness	**Cost**	**Creates other issues**	**Weakness**
Legal documents	Low - Medium	Low	Yes - confusion	Most players never read them
Stronger authentication	Medium - High	Medium - High	No	Players assume absolute safety
Detection and response	High	Medium	No	-
Monitoring players	High	Medium	Yes - privacy	-
Educating players	Medium	Low	No	Many players do not care until they become a victim
Regular updates	High	High		
Victim support	High	Medium - High	No	-

6.1 PROBLEM AREAS

The problem areas can be extracted from the second table, and are mostly in the weaknesses of the protection methods being used and the new issues that are being created when solving security issues.

Legal documents are supposed to tell players about the rights they have when playing a game, and what actions are prohibited. The e-commerce Directive (ECD)[28] dictates online game operators to show these Terms and Agreements to their customers, and to give them the option to either accept or decline them. The problem here is not only that the majority of the players never actually reads any of these Terms and Agreements, but also that they are quite often infested with vague, unclear and ambiguous language, open to many interpretations. The result of this is that players are unaware of what their rights and limitations are when playing an online game. Players generally know that they are not allowed to cheat, because it is unfair to their peer players. But they cannot always tell if and when their actions are classified as cheating, because there are many interpretations of what cheating is, not only between players, but also between game operators.

Another problem is online game operators pushing too far in their efforts to make their game secure. Invading the privacy of millions of players is a huge issue. By accepting the Terms of Use and the EULA, all of these players have agreed to this type of monitoring though, and as long as none of them successfully contests this particular part of the ToU and EULA in court, it is allowed. Sony BMG pushed it too far with the backdoor root kit software they shipped with their music CDs, and got corrected in court, but where exactly do we draw the line? If this kind of monitoring is accepted, it might very well become the standard, and then we can only wait to see what the next privacy invading step of these almighty companies is, all for the sake of protecting the security of their software, of course.

The weaknesses of stronger authentication and educating players are there because players don't care about security, or only start caring about it when it's already too late. The problem here is not with the technology or the effort people put in, but with the ignorance of players themselves. Many players only start to realize the emotional as well as monetary value of their game accounts once they lose them, and then it is too late, unless the game operator cleans up the mess for them, hoping they will at the very least learn to be more careful in the future. An account being compromised is not as bad as the related issue of identity theft, but it is an important topic nonetheless. Together with cheating related to virtual assets, it is the biggest security issue online games deal with, and the solution lies for the biggest parts in the hand of the players themselves.

6.2 Room for Improvement

Now, once we have indicated the problem areas, we can start talking about improvements to be made.

On the topic of legal documents, several improvements can be suggested. The first one is in the reform of the legal framework on electronic consumer contracts. The customer should be put central here, and vague, unclear and ambiguous language in customer contracts such as Terms of Use and End User License Agreements should be banished. This reform is a currently ongoing process. Question is however if the approach used in this process is the right one, and Christine Riefa indicates to be afraid that it is not, because some critical areas are left completely untouched, and a blueprint for the formation of e-contracts is not provided [15].
A second improvement I would like to suggest is about when and how a ToU and EULA are being presented. You cannot get around the obligation to show them and have them accepted before allowing access to the game for the first time, but after installing a new game, the last thing a player is interested in at that moment is reading several boring documents, which he can barely understand. During the installation process of a game there is a lot of time to show these

[28] http://ec.europa.eu/internal_market/e-commerce/directive_en.htm

contracts to a player, for example by showing one to players relevant clause in clear and unambiguous wording every minute or so. This still does not make sure they actually read them, but it at least gives them more opportunity to do so. After a game has been patched on the client side, players once again get the entire ToU and EULA showed to them, with the option to agree or decline. Would it not be a better idea to, after players have agreed to the contracts once, simply refer to them by providing a link to a website with these contracts, and only explicitly show clauses that were added, changed or removed? Maybe the legal framework on customer contracts does not allow this, but then this suggestion is just another issue to consider in its reform.

It is difficult to make player more aware of their account's security when they do not care about it. A solution is to create even more channels through which they are warned about security issues. You do not want to push the creation of awareness too far though, to a point where players become aware that they are playing a game that is not fun anymore because they are constantly spammed about security. Maybe more emphasis can be laid on security issues. Make the login screen *tip of the day* exclusively about security, replacing all the game play tips with security tips. Making authenticator tokens obligatory might increase overall account security, but might very well also decrease the amount of subscribers to an online game, and thus such measures must be evaluated with caution before implementing them.

A lot of small changes to protect security of online games can be made, and are made. On the player side, using a secure, up-to-date web browser with a plug-in that disables scripts from being executed by (potentially unsecure parts of) websites already makes a big difference. Advertisements for example can be disabled or completely hidden, and thus be prevented from executing potentially malicious scripts. Online game operators already warn that players should not give their login details to anyone, even if they think they are dealing with a game operator employee. They try to tell players how to distinguish between 'real' links in e-mails and fake ones. Maybe it is better to refrain from using links in e-mails at all, so that players who are aware of phishing activities are less likely to click on a link to a malicious website at all.
In World of Warcraft, a live chat with a game operator employee exists in such a way that attackers can't reproduce it, so that a player always knows whether or not he is talking to a legitimate employee. These kind of small changes can go a long way in ultimately reducing the amount of compromised account cases.

7 SUMMARY

In this thesis I have answered the five questions that I introduced in the introduction. The first question is answered in chapter 2; security in online gaming is needed for several reasons. These reasons include the massively distributed client-server architecture, mainly used in massive multiplayer online games, that has many vulnerabilities. Then there is the financial impact of many of such games, with in-game economies with which real-world profits can be made. Millions of gamers are willing to pay for playing an online game for years as long as it remains fair and protects them against threats from the inside and threats from the outside. Finally, there are the laws around online games that are still very dodgy and open to challenge in the developing fields of cybercrime, copyright and e-commerce.

In chapter 3, a list of the security issues online games and their players face is provided. The issues are taken from a framework made by Yan and Randell [7], and are divided into three categories; cheats, attacks and issues that can be executed both as a cheat and as an attack. Definitions for these terms are introduced in this chapter as well.

Chapter 4, then, attempts to provide a classification of the issues listed in chapter 3, together with a security analysis of these issues. The issues are compared on a variety of features; whether or not the issues are exclusive to gaming, how relevant the issues are to MMOs and other online games, who the offender and victim of each issue is, the vulnerability that is being exploited, the impact of the issue, the probability of the issue occurring and finally whether or not an issue can have legal consequences for the offender(s).

In chapter 5 I have described the various methods of protection online game operators apply to safeguard their games against cheaters and attackers, and I chapter 6 I review these protection methods. I indicate which of the issues are supposed to be dealt with by which methods. Then I discuss the effectiveness of these methods, their relative cost, the weaknesses they might have and whether or not they might create new issues in the progress of attempting to deal with security issues. Finally in this chapter, I discuss problem areas in the security of online gaming, and talk about improvements that could be made to this security.

8 Conclusions

By combining the answers to the five questions I asked in the introduction, I can now answer the main research question of this thesis: *what is the current state of the security in online gaming?*

As I discussed, one of the biggest security issues of games, namely piracy, almost completely disappears when the majority of the game play of a game requires interaction with a central server, which is the case in MMOs. One can steal and copy the client software, but in many cases this client software is already freely distributed by the game company. Instead of selling you the game, they sell you accounts to access the game.

To answer the second question; *which security issues are present within and around online gaming,* I originally intended to take the framework by Yan and Randell [7], because it was the most recent and complete one of the three frameworks I compared. While working with the framework however, I noticed how it was not only limited in the individual descriptions of the issues, but also a bit sloppy in general. I therefore made several improvements upon the framework. Classifying security issues in online games does however remain tricky, because there still is no one definition of cheating behaviors that is generally accepted. This is due to several reasons:

- Different game companies use different criteria to define cheating behaviors, making it more difficult but not impossible to talk about online gaming security issues in a general sense;
- Different types of games lead to different forms of cheating behaviors;
- Cheating in online gaming is a topic that is not yet widely explored by researchers;
- New cheats constantly rise as security companies and game companies defend older cheats, resulting in an arms race.

Nevertheless, I believe that the classification of security issues has its uses. It is always useful to think about potential weaknesses of software, whether you are a security analyst, an online game operator or just a gamer. It can help when you are creating a new game, to identify what issues are going to be relevant to the type of game you are designing. This way, you can attempt to deal with these issues in an early phase of the implementation. It can help players of a game to know how their peer players could try to gain an unfair advantage over them, or how attackers can try to steal their accounts.

Something I have added over most, if not all literature in the field of online gaming security, is a listing and review of various protection methods and security tools online game operators use to safeguard the security of their game, and to make sure people keep playing. Some authors talk about legal documents and the monitoring of players' computers [1], or briefly touch upon strengthening the authentication [2], but do not attempt to provide a more extensive listing of methods being used. It is however arguable how viable it is to score protection methods in a way as general as I have done. Ultimately, it is probably a far better idea to do this per game type, or even per game.

I mention Blizzard Entertainment often, not because of a bias, but because their game World of Warcraft is the best example of a game to be found when talking about security issues, both because of the type of the game and its popularity worldwide. Blizzard has a lot of experience when it comes to online gaming. Where their first games with online modes (Diablo and Diablo II) were infested with cheaters, to a point where you had to cheat not to gain an unfair advantage but to not be disadvantaged, they learned their lessons and improved in later games. Most game companies often have to push for deadlines and deliver unfinished software to survive in the

industry, resulting in the security issues not getting as much attention as they deserve. These issues are then left to be fixed in patches and other updates to the games.

Classic security terms as confidentiality, integrity, availability and privacy do play their roles in online game systems as they do all software systems that are developed these days. When talking about cheating however, *fairness* plays an important role as well. Fair play is something that is essential to any game, including online gaming. Because social structures that prevent or discourage unfair play are not or barely present in online environments, where people hardly know each other, security becomes important to enforce this fairness.

When it comes to the bigger tournaments for competitive online games, these still take place in locations where the players are put close to each other, and in most cases hardware – excluding keyboards and mouses – is supplied. Part of this is control of the tournament organizations, but enforcing fairness and thus security plays a big role here as well. Because of this, player skill is not the only requirement for gamers who want to participate in tournaments, the location puts an additional constraint; not every gamer has the ability and the resources to just move to Europe, the United States or even South Korea or even settle there.

Overall, I think the state of the security in online gaming is alright. As long as game companies (keep) try(ing) to learn from their own mistakes as well as from the mistakes of others, security issues can be combated adequately. When it comes to cheating, there is an ongoing arms race between online game operators and cheating players that will probably never completely be resolved. The biggest security issues cheating related to virtual assets and compromised accounts. They both are for the biggest part not the responsibility of online gaming companies, as dealing in virtual items outside the game is against the EULA of most games, and compromised accounts are often a result of carelessness on the side of the player. Assisting players who have had their accounts compromised of course is important to these companies, as a lack of service on that issue will most likely make many players decide to leave the game.

BIBLIOGRAPHY

[1] Greg Hoglund and Gary McGraw, *Exploiting online games: cheating massively distributed systems*, 1st ed.: Addison-Wesley Professional , 2007.

[2] Y-C Chen, P Chen, R Song, and L Korba, "Online Gaming Crime and Security Issue Cases and Countermeasures from Taiwan," in *2nd Annual Conference on Privacy, Security and Trust*, Fredericton, New Brunswick, Canada, 2004.

[3] Bruce Sterling Woodcock. MMOGCHART.COM 23.0. [Online]. http://www.mmogchart.com

[4] Gary McGraw and Ming Chow, "Securing Online Games - Safeguarding the Future of Software Security," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 11-12, May/June 2009.

[5] Matthew Pritchard. (2000, July) Gamasutra. [Online]. http://www.gamasutra.com/view/feature/3149/how_to_hurt_the_hackers_the_scoop_.php

[6] Henry Been-Lirn Duh and Vivian Hsueh Hua Chen, "Cheating Behaviours in Online Games," in *Lecture Notes in Computer Science 5621*. Berlin Heidelberg: Springer-Verlag, 2009, pp. 567-573.

[7] Jeff Yan and Brian Randell, "An Investigation of Cheating in Online Games," vol. 7, no. 3, pp. 37-44, May/June 2009.

[8] Jianxin Jeff Yan and Hyun-Jin Choi, "Security issues in online games," *The Electronic Library*, vol. 20, no. 2, pp. 125-133, 2002.

[9] Jeff Yan, "Security design in online games," in *Proceedings of the 19th Annual Computer Security Applications Conference*, 2003, pp. 286-297.

[10] Stephen Bono, Dan Caselden, Gabriel Landau, and Charlie Miller, "Reducing the Attack Surface in Massively Multiplayer Online Role-Playing Games," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 13-19, May-June 2009.

[11] N.E. Baughman and B.N. Levine, "Cheat-proof playout for centralized and distributed online games," in *Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, Anchorage, AK, USA, 2001, pp. 104-113.

[12] Meiring de Villiers, "Distributed Denial of Service: Law, Technology & Policy," *World Jurist Law/Technology Journal*, vol. 39, no. 3, 2006.

[13] Woodrow Barfield, "On money, taxes and property in virtual reality," *Virtual Reality*, vol. 13, no. 1, pp. 37-39, June 2008.

[14] Nicole van der Meulen and Bert-Jaap Koops, "The Challenge of Identity Theft in Multi-level Governance," *TILT Law & Technology Working Paper*, vol. 12, August 2009.

[15] Christine Riefa, "The Reform of Electronic Consumer Contracts in Europe: Towards and Effective Legal Framework?," *Lex Electronica*, vol. 14, no. 2, September 2009.

[16] Tsun-Yu Hsiao and Shyan-Ming Yuan, "Practical Middleware for Massively Multiplayer Online Games," *IEEE Internet Computing*, vol. 9, no. 5, pp. 47-54, September/October 2005.