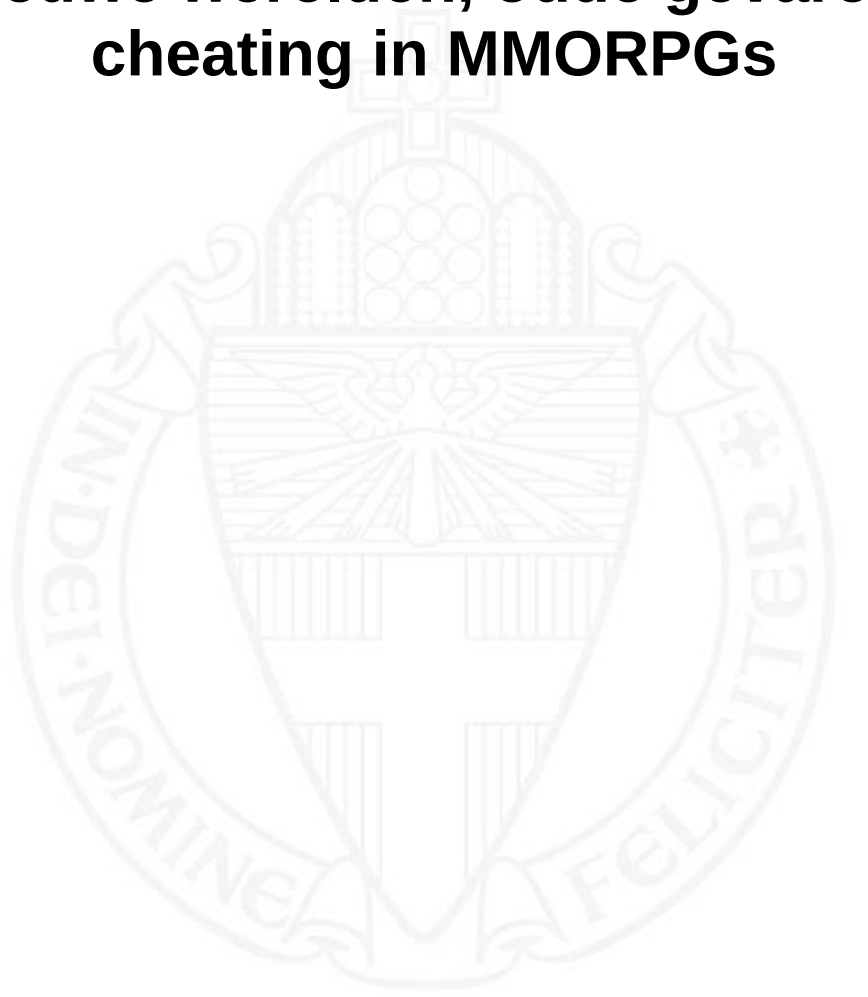
Nieuwe werelden, oude gevaren: cheating in MMORPGs



Radboud Universiteit Nijmegen

Bachelorscriptie Informatiekunde

Begeleider:	**Prof. dr. B.P.F. Jacobs**
Coördinator:	**Dr. S.J.B.A. Hoppenbrouwers**
Auteur:	**Alex Hamakers**
Datum:	**Juni 2006**
Studentnummer:	**S0115541**
Studie:	**Informatiekunde**

Voorwoord

Gamen neemt een steeds grotere plek in in de entertainmentmarkt. De opkomst van het internet heeft ervoor gezorgd dat een keur aan nieuwe genres is ontstaan met online multiplayer-mogelijkheden. Een specifiek genre heeft in korte tijd ontzettend aan populariteit gewonnen: de MMORPG; oftewel de ‘Mass Multiplayer Online Role Playing Game’. In deze games bevinden duizenden gamers zich tegelijk in dezelfde immense online wereld. Samen gaan ze de strijd aan met grote monsters of vechten ze onderlinge oorlogen uit. Geen zin in vechten? Dan kan er een nieuwe uitrusting bij elkaar gezocht worden, of je begint een handeltje in grondstoffen, wapens en magische spullen.

Zelf heb ik menig uur in zo’n virtuele wereld doorgebracht. Ik raakte steeds geïnteresseerder in het gebeuren eromheen: hoe werkt het, wat zijn problemen waar men tegen aanloopt en hoe worden deze opgelost? Zodoende kwam ik uit bij het onderwerp van deze scriptie: cheating in MMORPGs. Dit onderwerp vormt een interessante koppeling tussen mijn hobby en mijn opleidingsgebied, waardoor ik het een geschikt onderwerp vind voor mijn bachelorscriptie.

Ik wil graag de heer Bart Jacobs bedanken voor zijn ondersteuning bij het schrijven van deze scriptie. Zijn inzichten in de wereld van software security en zijn gezonde niveau van paranoia ten opzichte van applicaties hebben mij erg geholpen bij het schrijven van deze scriptie. Ten slotte wil ik Judith Coenen bedanken voor het verbeteren en controleren van deze scriptie op het gebied van spelling en grammatica.

Inhoudsopgave

1. Nieuwe werelden, oude gevaren

Helaas is geen enkele wereld perfect en vrij van kwaadwillenden, zo lopen er ook in de virtuele wereld van de MMORPG oplichters, valspelers en pestkoppen rond die het plezier van anderen verpesten. Deze mensen worden ook wel cheaters genoemd. Deze cheaters maken gebruik van bugs in de games of speciale cheatprogramma's om een oneigenlijk voordeel te behalen. Iedereen kan zich voorstellen dat zowel de producenten van MMORPGs als eerlijke gamers hier niet op zitten te wachten, zeker niet als ze per maand moeten betalen om deel te mogen nemen aan een game. Hierom maken producenten gebruik van verschillende methodes om cheaters aan te pakken. In games zie je dezelfde ontwikkelingen als in de hackerswereld of de criminaliteit: als er regels en wetten worden gemaakt, dan worden de nieuwe mazen gezocht. Een van de laatste ontwikkelingen op het gebied van anti-cheatmethodes zijn aparte programma's die apart van de game draaien om cheaters op te sporen. Deze programma's worden niet met veel enthousiasme ontvangen, omdat ze er voor gemaakt zijn om gebruikers in de gaten te houden. Zodra gebruikers gecontroleerd worden volgt de discussie over de privacy van de consument.

De problemen met cheaters worden steeds groter door verschillende oorzaken. Vroeger waren MMORPGs niet heel 'mass' en bleef de gebruikersgroep vooral beperkt tot de hard core gamers. Met de komst van 'World of Warcraft' en andere grote namen begon het genre snel te populariseren (Wikipedia, 2006). Vergelijk het met de ontwikkeling van internet. In het begin was het internet vooral een speeltje voor techneuten en geïnteresseerden, maar het internet begon pas echt te groeien toen het ontdekt werd door de massa. Deze ontwikkeling ziet men ook bij de MMORPGs, er komen steeds meer nieuwe gamers bij. Al deze nieuwe gamers brengen nieuwe problemen met zich mee: de hard core fans zijn al thuis in het wereldje en bewuster van de bestaande problemen met cheaters. Ze zijn minder vatbaar zijn voor cheaters en fraudeurs omdat ze in ieder geval al van het bestaan ervan afweten. Nieuwe gamers stappen vaak nietsvermoedend een digitale wereld binnen die op het eerste gezicht erg beschermend is. De wereld bevindt zich op servers van de producent zelf, deze zal toch wel voor bescherming zorgen? Helaas is dat niet altijd het geval, en al snel komen ze er achter dat ook in de virtuele wereld alle soorten mensen vertegenwoordigd zijn, dus ook de kwaadwillenden.

Met het groeien van de markt nemen ook de mogelijkheden tot opbrengsten toe. Wil je deel kunnen nemen aan bijvoorbeeld World of Warcraft (de populairste MMORPG van het moment), dan moeten er naast het aankoopbedrag van zo'n 45 euro ook maandelijkse abonnementskosten betaald worden, tussen de 10 en de 15 euro (afhankelijk van de afgenomen hoeveelheid maanden). Games als project Entropia gaan nog een stapje verder: daarin bestaat een echte economie en moet er geld betaald worden voor content (inhoud zoals wapens, huizen of kleding). Zo is het mogelijk om een winkel in de wereld te beginnen, maar daar moet dan wel echt geld voor betaald worden aan de producenten. Vervolgens kunnen ze in deze winkel weer producten voor echt geld verkopen. Op deze manier zijn er mensen die daadwerkelijk hun geld verdienen door virtuele spullen in een virtuele omgeving te verkopen.

Doordat meestal betaald moet worden voor MMORPGS verwachten de klanten ook meer dan alleen een spelomgeving op een server waarin ze hun virtuele leven kunnen leiden. Ze verwachten dat ze beschermd worden door de producent en dat ze niet gedupeerd worden door cheaters. Er is dus een extra verantwoordelijkheid bijgekomen en de vrijblijvendheid van het aanbieden van de dienst is verdwenen. Waar in eerdere games nog wel eens de hele economie ontregeld kon worden door cheaten is dat tegenwoordig volstrekt ontoelaatbaar. Schadeclaims kunnen dan ook verwacht worden wanneer de virtuele wereld zodanig verpest wordt dat klanten daadwerkelijk geld verliezen.

2. Onderzoeksvraag

Het onderzoeksgebied van deze scriptie is cheats in MMORPGs. Hierbij wordt de focus gelegd op welke methodes er op het moment ingezet worden om cheaten tegen te gaan en wat daar de sterke en zwakke punten in zijn. Dit valt samen te vatten in de volgende onderzoeksvraag:

"Wat zijn de sterke en zwakke punten van de manieren waarop cheaters in MMORPGs worden opgespoord?"

Deze onderzoeksvraag kan opgedeeld worden in verschillende deelvragen waarop eerst een antwoord gegeven dient te worden voordat onderzocht kan worden waar de sterke en zwakke plekken. Ten eerste moet helder en duidelijk gespecificeerd worden wat wel en wat niet onder cheaten valt. Mensen zoeken immers altijd de grenzen van het toelaatbare op en of iets al dan wel of niet acceptabel is hangt vooral af van de gekozen definitie. Om te kunnen beoordelen wat goed en slecht is aan een methode moet eerst duidelijk zijn wat deze methode precies tegen moet gaan. De eerste deelvraag waarop antwoord gegeven moet worden is:

"Wat is een goede definitie van cheaten?"

Het antwoord op deze vraag is nog vrij algemeen en beschrijft cheaten in zijn algemeenheid. De definitie is dus ook te gebruiken voor singleplayer games waarbij de gamer het in zijn eentje opneemt tegen de computer. Deze definitie is te breed om daadwerkelijk gebruikt te kunnen worden om methodes te beoordelen. Hij moet dus toegespitst worden op het specifieke onderwerp cheaten in MMORPGs. Deze definitie is het antwoord op de volgende deelvraag:

"Wat is een goede definitie van cheaten in MMORPGs?"

Als deze definitie gegeven is kan verder onderzocht worden op welke manier er gecheat wordt in MMORPGs:

"Op welke manieren wordt er gecheat in MMORPGs?"

Als duidelijk is wat het probleem precies is kan de aandacht verplaatst worden naar de methodes die ingezet worden om cheaten tegen te gaan. Maar voordat de methodes besproken worden moet er een manier zijn om ze te kunnen beoordelen, anders kunnen er namelijk geen zwakke plekken en sterke punten ontdekt worden. De deelvraag die hierbij hoort is:

"Op welke manier kunnen methodes beoordeeld worden?"

Door het combineren van de inzichten die verkregen zijn door de opgestelde definities, het bestuderen van de huidige problemen en het opstellen van de beoordelingsmethodes kunnen de methodes onderzocht en geanalyseerd worden. Na deze analyse moet het mogelijk zijn om de onderzoeksvraag te beantwoorden.

3. Onderzoeksmethode

3.1. Theoretisch kader

Deze onderzoeksvraag bevindt zich in verschillende kennisgebieden:

Informatica

MMORPGs spelen zich op internet af, cheaters maken gebruik van vernuftige programma's om te cheaten en fabrikanten gebruiken vernuftige programma's om cheaters op te sporen. Deze programma's zullen onderzocht en beoordeeld moeten worden om een antwoord te vinden op de onderzoeksvraag

Sociologie

Wat is een cheater? Wie heeft er last van en welke impact hebben ze op het gameplezier? Een anti-cheatmethode kan zeer effectief zijn, maar als deze methode normale gamers het plezier ontneemt schiet men weinig op.

Juridisch/ethisch

Internet is juridisch gezien een grijs gebied en sommige anti-cheatmethodes hikken tegen het randje aan van legaliteit. Er moet bijvoorbeeld ook rekening worden gehouden met de privacy van de gamers.

3.2. Strategie

Opbouw van de scriptie

Zoals te zien is in het vorige hoofdstuk is de onderzoeksvraag opgesplitst in verschillende deelvragen. Dit is niet alleen gedaan om het overzicht te bewaren maar ook om de opbouw naar het uiteindelijke antwoord inzichtelijk te maken. Eerst worden de fundamenten gelegd (waar gaat het nu precies over, waar kan het mee vergeleken worden, wat is relevant, en wat niet?). Daarna kunnen de verschillende onderdelen met elkaar gecombineerd worden zodat er een conclusie uit getrokken kan worden. Door de losse en elementaire stappen is het redeneerproces goed te volgen en zitten er geen logische gaten in de redenering.

Het verzamelen van de informatie

De informatie die voor de scriptie gebruikt wordt komt uit verschillende bronnen. Sommige wetenschappelijk, andere niet. Omdat de wereld van de games vrij nieuw is, is er nog vrij weinig wetenschappelijk verantwoord onderzoek over te vinden. Informatie over het ontstaan van cheats en informatie over de manier waarop cheaten momenteel wordt aangepakt zal dan ook gezocht moeten worden op internet. Bij het verzamelen van deze informatie moet de betrouwbaarheid goed in de gaten gehouden worden. De correctheid van de gegevens kan ik grotendeels waarborgen door mijn achtergrond. Doordat ik de wereld van de games van binnen en van buiten ken en al langer vanuit verschillende perspectieven bekijk kan ik een goede inschatting maken van de correctheid en de waarde van de gevonden informatie.

3.3. Antwoord

Het antwoord op de deelvragen *"Wat is een goede definitie van cheaten?"* en *"Wat is een goede definitie van cheaten in MMORPGs?"* zullen definities zijn. De deelvraag *"Op welke manieren wordt er gecheat in MMORPGs?"* levert als antwoord een analyse van de zwakke plekken in MMORPGs en op welke manieren cheaters daar misbruik van maken. De deelvraag *"Op welke manier kunnen methodes beoordeeld worden?"* levert een lijst met aspecten op waarop methodes beoordeeld kunnen worden. Per aspect kan aangegeven worden hoe de methode op dat gebied scoort. De mogelijke scores zijn +, 0 en -. Dit is een vrij eenvoudig beoordelingsysteem, maar meer is ook niet nodig om sterke en de zwakke plekken aan te geven.

Het antwoord op de onderzoeksvraag *"Wat zijn de sterke en zwakke punten van de manieren waarop cheaters in MMORPGs worden opgespoord?"* wordt geleverd door de antwoorden uit de deelvragen te combineren. Door het beantwoorden van de deelvragen is duidelijk wat het probleem precies is, wat eraan gedaan wordt en wat daar de sterke en zwakke punten in zijn. Al deze informatie wordt geanalyseerd zodat er uiteindelijk een conclusie aan verbonden kan worden. Met die analyse en conclusie is de onderzoeksvraag beantwoord

4. Het onderzoek

4.1. Wat is cheaten?

Het woord cheaten heeft veel verschillende vertalingen naar het Nederlands. Het betekent niet alleen vals spelen, maar bijvoorbeeld ook vreemdgaan, spieken, bedriegen, of iemand erin luizen (Wordnet, 2006). De gemeenschappelijke factor die al deze termen verbindt is dat iemand die cheat afwijkt van de gestelde regels. Het begrip regels kan hierbij ruim opgevat worden. Het kan geïnterpreteerd worden als de regels van het spel, maar ook als de examenreglementen, de sociale omgangsvormen of zelfs de wet. In games is het de vraag volgens wiens regels er gecheat wordt. Zijn het algemene normen en waarden, of worden alleen de regels van de producent geschonden? De eerste stap die genomen wordt om een goede definitie van cheaten op te kunnen stellen is het analyseren van de geschiedenis van cheaten. Daarna wordt onderzocht op welke manieren gecheat wordt, zodat er een compleet beeld ontstaat van de verschillende soorten. Het moeilijke aan het opstellen van de definitie is dat de opinie over wat cheaten is steeds verschuift. Sommige methodes worden na loop van tijd geaccepteerd als legitieme methodes om het gamen gemakkelijker te maken, terwijl er aan de andere kant nieuwe manieren ontstaan om te cheaten. Het cheat probleem is een zogenaamd moving target. Een opgestelde definitie moet daar op inspelen door aan de ene kant niet te specifiek te zijn in het benoemen van de methodes en aan de andere kant ook alle mogelijke nieuwe cheatmethodes af te vangen.

4.1.2. Cheaten: duizend-en-één manieren

Cheaten is een term die ongeveer tegelijkertijd met het gamen is geïntroduceerd. Zodra er games op de markt verschenen ontstonden er cheats om deze games op een ‘oneerlijke’ manier te beïnvloeden. Waarom oneerlijk tussen haakjes? In vele games kan er gecheat worden, maar op een oneerlijke manier het spel beïnvloeden suggereert dat iemand anders er nadeel van ondervindt. In tegenstelling tot de meeste gezelschapspellen waarin het vals spelen is uitgevonden, werden de eerste cheats gebruikt in singleplayer games. Singleplayer betekent dat iemand tegen de computer speelt en niet tegen een andere speler. Hierbij kan de computer/kunstmatige intelligentie de rol van een andere speler op zich nemen of alle vijanden aansturen. Als er gecheat wordt in single player games ondervinden andere gamers hiervan niet direct negatieve invloed, aangezien er geen slachtoffer is als een speler vals speelt tegen de computer. De zaak verandert echter wanneer er gecheat wordt in multi player games. Nu heeft de ene speler namelijk een oneerlijk voordeel ten opzichte van de andere, aangezien de cheater het spel zodanig aanpast dat hij een oneerlijk voordeel heeft ten opzichte van de medespeler.

De eerste cheat ooit werd gevonden in de game ‘Adventure’ voor de Atari 2600, een adventure game die uitkwam in 1978 (Wikipedia, 2006). Net als bij films wordt tegenwoordig bij games na afloop een aftiteling getoond waarin alle betrokkenen genoemd worden. Bij Atari destijds echter nog niet. Warren Robinett, een van de gamedesigners vond dat hij hierdoor niet de eer kreeg die hem toekwam, daarom stopte hij een easter egg in de game. Een easter egg is een onschuldig extra stukje programma dat na goed zoeken ontdekt kan worden. Een beroemd voorbeeld is het racespelletje dat verstopt zit in Excel en gespeeld kan worden door het maken van een reeks onlogische acties. In Adventure kon de easter egg ontdekt worden door in de game een onzichtbare pixel te verschuiven waardoor een geheime kamer geopend werd. In die geheime kamer was: “Created by Warren Robinett” op de vloer geschreven Zo kreeg Robinett toch nog de eer en aandacht die hem volgens hemzelf toekwam.

In de loop van de tijd zijn er verschillende methodes om te cheaten ontstaan. Sommige zijn bewust door de fabrikant in de game geplaatst om de gamer extra mogelijkheden te geven, andere zijn ontstaan door slordigheden van de fabrikant of door inventieve gebruikers die de zwakke plekken van een game opzoeken en deze misbruiken om te cheaten. Ik maak een onderscheid tussen vijf hoofdcategorieën van cheatmanieren waarmee de meeste cheatmethodes zijn afgevangen.

4.1.3. Codes

Een bekende manier van cheaten is het gebruiken van codes om onkwetsbaar te worden of om hele stukken van een game over te slaan (Wikipedia, 2006). In PC-games worden deze codes vooral via het toetsenbord ingegeven, in console game worden vooral knoppencombinaties gebruikt. Cheat codes zijn ontstaan omdat programmeurs speciale codes in software stopten waardoor testers gemakkelijk de hele game konden testen. Hoe moest men anders het laatste level testen, als de tester te slecht was om tot het laatste level te komen? Deze codes zorgen ervoor dat het startlevel gekozen kan worden, de speler oneindig veel levens meekrijgt of onkwetsbaar wordt. Programmeurs zijn echter af en toe slordig en vergeten deze codes uit de game te halen voordat deze op de markt gebracht wordt. De codes die eigenlijk bedoeld zijn om de game te kunnen testen worden dan door gebruikers gebruikt om moeilijke stukken over te slaan of om onkwetsbaar te worden: cheaten.

4.1.4. Het aanpassen van user settings of de interface

De meest eenvoudige manier van cheaten is het aanpassen van de instellingen. Het aanpassen van de instellingen wordt mogelijk gemaakt door de producent zodat de game aangepast kan worden aan de wensen van de gebruiker. Niet alleen de knoppen kunnen toegewezen worden, in PC-games is het bijvoorbeeld ook mogelijk om op grafisch gebied van alles aan te passen. Het directe voordeel wordt dan bijvoorbeeld behaald door de brightness zodanig omhoog te schroeven dat donkere gebieden geen gezichtsbelemmering meer opleveren. Het wordt dan al een stuk makkelijk om tegenstanders te ontdekken aangezien ze zich niet meer kunnen verstoppen in donkere hoekjes. Een andere manier is het aanpassen van de textures waardoor de tegenstanders niet meer in camouflagekleding rondlopen maar in een goed zichtbaar kerstmannenpakje. Omdat deze aanpassingen binnen de gestelde grenzen van de game gebeuren worden ze niet echt als cheaten gezien, ook al wordt er voordeel mee behaald.

In MMORPGs past zelfs bijna iedereen de interface aan. De standaardinterface bevat volgens veel mensen niet genoeg informatie en die passen hem dan ook graag aan. Binnen de game zelf bestaan hier vaak mogelijkheden toe, maar vaak kunnen er extra programma's geïnstalleerd worden om de interface aan te passen. Opmerkelijk is dat niemand dit als cheaten beschouwd maar als een legitieme manier om de game beter te kunnen spelen. Dit is dan ook een goed voorbeeld van de verschuivende opvattingen over wat cheaten is. Vroeger waren de meningen verdeeld over of het toegestaan is om interfaces aan te passen maar nu is het vrij geaccepteerd.

4.1.5. Externe software

Als externe software gebruikt wordt om te cheaten dan draait deze meestal tegelijkertijd met de game. De externe software wordt gebruikt om de cheater te helpen bij het spelen van de game. Een voorbeeld zijn de zogenaamde aim-bots. Deze programmaatjes worden vooral gebruikt in shooters, waarbij het van belang is om zo secuur mogelijk te richten. Een aim bot ondersteunt dit door de positie van een tegenstander te bepalen en hier dan het richtpunt naartoe te bewegen. Hierdoor hoeft de gamer zelf niet meer te richten en schiet hij altijd raak.

Ook in console games komt deze vorm van cheaten voor. Dit werkt op een andere manier dan cheaten in PC-games, omdat op consoles geen extra software kan worden geïnstalleerd. Bij consoles bestaat er een fysieke scheiding tussen de soft- en de hardware. Games staan op schijfjes of cartridges en de hardware bevindt zich in de console. Voor consoles worden speciale cheatapparaten uitgebracht die meestal fysiek tussen soft- en hardware worden geplaatst. De cheattool bevindt zich dan in principe in de communicatie van soft- en hardware en past daar de data aan. Lezers die bekend zijn met de security-wereld kunnen hierbij denken aan een man-in-the-middle attack.

4.1.6. Cheaten via de connectie

Het plotseling sluiten van de verbinding kan op verschillende manieren gebruikt worden om te cheaten. Sommige games werken met een (wereldwijd) rankingsystem (Wikipedia, 2006). Hoe meer wedstrijden er gewonnen worden, hoe hoger de plaats op deze ranglijst wordt. Verloren wedstrijden kunnen ervoor zorgen dat iemand daalt op de ranglijst. Wat kun je doen als je aan de verliezende hand bent en er voor wil zorgen dat je eigen plaats behouden wordt en de ander niet stijgt? Disconnecten voordat de ronde is afgelopen waardoor er niemand als winnaar of verliezer geregistreerd wordt. Deze zijn namelijk nog niet bekend als de wedstrijd voortijdig beëindigd wordt. Een manier om dit tegen te gaan is door ervoor te zorgen dat iemand die de verbinding verbreekt automatisch als verliezer wordt bestempeld. Maar hier zijn weer mensen die last hebben van een instabiele verbinding hebben extra de dupe van, zij kunnen het gevoel krijgen dat ze extra gestraft worden. Specifieke manieren waarop het knoeien met de verbinding gebruikt wordt in MMORPGs worden verderop behandeld.

4.1.7. Oplichting

Als een game bestaat uit interacties tussen verschillende mensen, dan ontstaat er ruimte voor oplichting, zeker als deze interacties bestaan uit handel. Dit wordt zoveel mogelijk voorkomen door allerlei restricties en veiligheidsmaatregelen, maar net als in de echte wereld weten oplichters in de virtuele wereld hun weg te vinden door de mazen van het net. Ik beschouw dit ook als cheaten omdat de ene speler een oneerlijk voordeel behaalt tegenover een andere speler. Oplichting is een reeël probleem in games, zeker als voorwerpen betaald worden met echt geld in plaats van met virtueel geld.

4.1.8. Wat is een bruikbare definitie van cheaten?

Het beeld van wat cheaten precies is verandert met de tijd, denk aan het aanpassen van interfaces. Er zijn echter bepaalde aspecten die iedere keer terug komen wanneer men spreekt van cheaten. Alvorens tot een definitie gekomen kan worden is het verstandig om deze aspecten op een rijtje te zetten. Een cheat wordt gekenmerkt door de volgende aspecten:

- Een cheat verandert de state van een programma of de view op deze state.
- Een cheat levert een voordeel op voor de cheater. Dit voordeel ontstaat doordat de cheater ofwel meer mogelijkheden krijgt in de game, of minder beperkingen heeft.
- Er bestaan verschillende manieren om te cheaten, en deze mogelijkheden nemen alleen maar toe doordat er steeds nieuwe manieren bedacht worden.
- Door het gebruiken van een cheat worden bepaalde regels geschonden, die opgesteld zijn door de fabrikant of regels die behoren tot de algemene gedachte van de gebruikersgroep over wat eerlijk gamen is.

Rekening houdend met deze aspecten van cheaten kan de volgende definitie opgesteld worden:

Cheaten is het behalen van een oneigenlijk voordeel door het veranderen van de state van een game of het veranderen van de view op deze state, waardoor impliciete of expliciete regels geschonden worden.

Dit is de algemene definitie van cheaten en bruikbaar voor zowel singleplayer en multiplayer games. Cheaten met bijvoorbeeld een code in een singleplayer game valt hier dus ook onder. Als iemand cheat met een code in een singleplayer game zal niemand daar bezwaar tegen hebben, de enige partij die er nadeel van ondervindt is de kunstmatige tegenstander die door de computer zelf gevormd wordt. In dit onderzoek draait het echter om cheaten in een omgeving waarin zich meerdere gebruikers bevinden die er wél nadeel van ondervinden. De volgende stap bestaat dan ook uit het aanpassen van deze algemene definitie van cheaten naar de specifieke situatie waar deze scriptie zich op richt: het cheaten in MMORPGs.

4.2. De zwakke plekken in MMORPGs

4.2.1. Een specifieke definitie van cheaten in MMORPGs

Bij het opstellen van een definitie van cheaten in MMORPGs moeten nog een paar andere aspecten meegenomen worden:

- Meerdere gebruikers zijn erbij betrokken. Wanneer er gecheat wordt in een MMORPG dan is hier altijd iemand anders de dupe van. Dit kan doordat de cheater oneerlijk voordeel heeft of doordat andere spelers er nadeel van ondervinden.

- Door het cheaten verkleint de cheater beperkingen of vergroot de mogelijkheden in vergelijking met andere spelers.

- Gecheat kan worden in de interactie tussen gebruikers maar ook door het beïnvloeden van de spelwereld.

- Producenten leggen meestal expliciet vast welke regels er gelden binnen een game en welke beperkingen. Dit document noemt men een policy. Deze policy is echter vrij aanpasbaar waardoor de mogelijkheid bestaat deze regels aan te passen aan de huidige situatie. Wanneer er een nieuwe cheatmogelijkheid wordt ontdekt dan wordt deze (meestal) afgedekt in de policy.

Met deze extra punten kan de algemene definitie van cheaten toegespitst worden op cheaten in MMORPGs:

Cheaten in MMORPGs is het behalen van oneigenlijk voordeel ten opzichte andere spelers door het onrechtmatig veranderen van de state van een game of het veranderen van de view op deze state, waardoor de eigen mogelijkheden vergroot of de eigen beperkingen verkleind worden. Deze mogelijkheden en beperkingen zijn impliciete of expliciet vastgelegd door de producenten of de gebruikerscommunity.

4.2.2. Cheaten in MMORPGs

In MMORPGs is één ding het allerbelangrijkst voor de spelers: het eigen karakter. In tegenstelling tot bijvoorbeeld shooters waarin het karakter een vrij anonieme rol vervuld is het karakter hét onderdeel van de MMORPG waar alles om draait. Het dient als avatar van de speler in de virtuele wereld en via deze avatar beleeft de speler alle avonturen. Als ieder karakter hetzelfde zou zijn zou de game al snel saai en onaantrekkelijk worden: iedereen wil uniek zijn en zich onderscheiden van de massa. MMORPGs voorzien hierin door een grote aanpasbaarheid van het karakter te bieden. De verschillen tussen de karakters die de virtuele wereld bevolken kunnen in essentie ingedeeld worden in drie categorieën: de eigenschappen van het karakter, de uitrusting en de directe aansturing. Doordat deze drie categorieën het verschil maken tussen de verschillende spelers proberen cheaters op een of meerdere van deze categorieën hun voordeel te behalen. Per categorie zijn er dan ook specifieke cheatmanieren te onderkennen die precies dát punt wat het karakter maakt proberen te beïnvloeden. In het volgende onderdeel worden de drie categorieën beschreven waarna per categorie aangegeven voor welke manier van cheaten (beschreven in sectie 4.1.) deze vatbaar is.

4.2.3. De eigenschappen van het karakter

Tegenwoordig is het mogelijk om het uiterlijk van een karakter helemaal in te stellen zodat iedere individuele speler er anders uitziet. Met dit karakter wordt meestal lange tijd gespeeld. Om te voorkomen dat een MMORPG saai wordt ontwikkelen karakters zich naarmate er meer mee gespeeld wordt: ze worden krachtiger, slimmer of leniger. Een speler die vooral veel met een zwaard vecht en de directe confrontatie aangaat zal beter worden in zwaardvechten en meer kracht ontwikkelen. Een speler die vooral sluipt en gebruik maakt van pijl en boog om zijn tegenstanders vanaf een afstand te belagen zal beter worden met pijl en boog. Doordat de ontwikkeling direct samenhangt met de tijd die met het karakter gespeeld wordt verschillen de karakters onderling in sterkte. Deze ontwikkeling zorgt ook voor de competitie tussen de verschillende deelnemers want iedereen wil natuurlijk de sterkste, de slimste, de lenigste en de beste zijn.

Vatbaar voor:

- **Externe software.** De eigenschappen van het karakter kunnen beïnvloed worden door het gebruik van externe software. Directe aanpassing van het karakter is erg moeilijk (wordt verder uitgelegd in alinea 4.2: het client-server model) omdat deze data zoveel mogelijk wordt afgeschermd. Als een gamer geen zin heeft om zelf uren in de ontwikkeling van een karakter te steken dan kan externe software worden ingezet. Deze software neemt dan de rol van de speler over en de speler kan iets anders gaan doen. In het merendeel van de MMORPGs worden karakters beter door het verslaan van vijanden. Om heel veel beter te worden moeten er vaak ontzettend veel vijanden doodgemaakt worden en dit kan op den duur erg saai worden. Het puur afmaken van vijanden om beter te worden wordt ook wel grinden genoemd. Omdat dit vechten vaak uit een steeds dezelfde combinatie van stappen bestaat kan dit relatief eenvoudig door een programma overgenomen worden. Dit programma spoort vijanden op en valt vervolgens aan volgens een vast patroon. Het karakter wordt zo sterker zonder dat de cheater er zelf veel tijd in hoeft te steken.

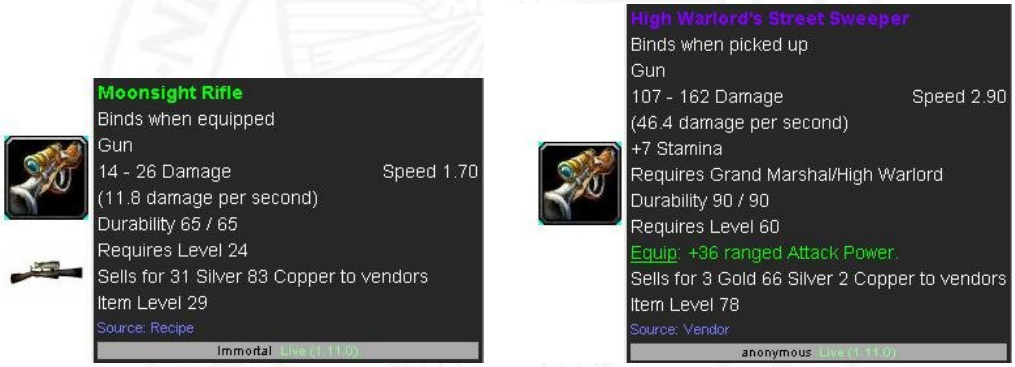
4.2.4. De uitrusting

Niet alleen de status van het karakter bepaalt de mogelijkheden: ook de uitrusting speelt een grote rol. Zo kan het gebeuren dat in een confrontatie tussen twee spelers die precies even lang gespeeld hebben en die hun karakter precies op dezelfde manier ontwikkeld hebben de een altijd de ander zal verslaan. Dit wordt veroorzaakt door de verschillen in uitrusting. De karakters in MMORPGs zijn uit te rusten met allerlei verschillende wapens, kleren, harnassen, ringen, magische items, enzovoorts. Deze items zorgen voor een verdere differentiatie van de verschillende karakters. Ook zorgen deze items voor een levendige handel in MMORPGs . Zo kan het voorkomen dat een zwaardvechter een magische staf vind waar hij niks mee kan. Hij laat dan weten dat hij in het bezit is van deze magische staf en zal hem waarschijnlijk aan de hoogste bieder of een bevriende speler verkopen. Dit zorgt voor een levendige handel in MMORPGs tussen de verschillende karakters. Het is niet ongewoon dat duizenden voorwerpen tegelijk aangeboden, gekocht en verkocht worden in een virtuele veilinghal.

Vatbaar voor:

- **Cheaten via de connectie.** Als men een manier heeft gevonden om een server te kunnen laten crashen (bijvoorbeeld door een bug of het creëren van een uitzonderlijke situatie), dan kan dit misbruikt worden om te cheaten. MMORPG-servers draaien meestal een real time wereld. Om te zorgen dat de gehele voortgang niet verloren gaat in een crash wordt de gehele wereld op bepaalde momenten gesaved. Karakters van afzonderlijke spelers worden iedere keer gesaved bij het afsluiten. Stel nu dat een speler een exclusief voorwerp heeft dat erg veel geld waard is en erg zeldzaam is. Hij geeft dit voorwerp aan een medespeler die daarna meteen uitlogt; Het karakter van de medespeler wordt dan gesaved. Als de oorspronkelijke bezitter er vervolgens in slaagt om de server te laten crashen zal deze de laatste back-up terugzetten, waarin de oorspronkelijke bezitter het voorwerp nog in zijn bezit heeft. Deze techniek valt ook wel onder de noemer “item duplication”.

- **Oplichting.** Cheaters weten ook aan een betere uitrusting te komen door andere spelers op te lichten. Dit kan door bijvoorbeeld een niet zo waardevol item aan een andere speler te verkopen en net te doen alsof het een veel waardevoller item is waardoor er meer voor betaald wordt. Met duizenden verschillende items komt het snel voor dat items veel op elkaar lijken waardoor verwarring ontstaat. Cheaters maken hier misbruik van door andere gebruikers die ter goeder trouw handelen op te lichten. Per game verschilt de precieze manier van oplichting en worden verschillende methodes gebruikt, maar het blijft een algemeen probleem in MMORPGs.



Het item rechts is meer dan tien keer zo waardevol als het item links. Maar wie ziet het verschil als bij de verkoop alleen de plaatjes in beeld komen?

4.2.5. De interactie

Het karakter wordt vooral gevormd door de kenmerken en de uitrusting, maar ook de vaardigheden van de speler dragen bij aan de mogelijkheden. Iemand die goed is in sluipen zal meer tegenstanders verrassen dan iemand die struikelt over iedere boomstronk. Ook is het vaak van belang welke aanval er ingezet wordt. Wordt er eerst een verlammende spreuk ingezet om daarna de aanval in te zetten of toch maar de verrassingsaanval met de meest vernietigende spreuken? Hoe goed het karakter is wordt dus ook beïnvloed door de manier waarop het direct bestuurd wordt door de speler. In theorie kan een karakter dat de beste uitrusting heeft en waarin al honderden uren zijn gestoken nog steeds verslagen worden door een nieuw karakter dat net is aangemaakt. In de praktijk wordt in MMORPGs op dit gebied niet zoveel gecheat aangezien het weinig effect oplevert, vergeleken met de moeite die gedaan moet worden. Toch werd er vroeger veel gecheat op het gebied van de interactie. Het gebeurde toen vooral door de verzonden data aan te passen. Veel cheatmogelijkheden worden al voorkomen door de architectuur van de games en door het beveiligen van de verbinding. Deze problemen worden toch even aangestipt voor de volledigheid.

Vatbaar voor:

- **Cheaten via de connectie.** Er is een mogelijkheid om op dit gebied te cheaten door de verzonden data aan te passen. Zo is het in sommige games bijvoorbeeld mogelijk om de veroorzaakte schade te verhogen of om te zien wat er zich achter een muur bevindt.

- **Externe software.** Externe software sluit meestal aan op het cheaten via de connectie, oftewel het aanpassen van de data. Hoewel het mogelijk is om bijvoorbeeld een programma te gebruiken dat helpt bij het richten is dit meestal niet zo bruikbaar in MMORPGs, omdat het verschil in een gevecht hierin niet gemaakt wordt door de precisie maar meer door de gevolgde strategie.

4.2.6. Waar zijn de codes en aanpassingen van de user interface?

Zowel het gebruik van codes en het aanpassen van de user interfaces zijn geen issue in MMORPGs. Per manier is hier een andere oorzaak voor. Cheat codes worden vaak bewust door fabrikanten ingebouwd in een game. Dit laten ze vanzelfsprekend achterwege als ze niet willen dat cheat codes in de game te vinden zijn. De codes die door programmeurs en testers gebruikt worden om snel door het hele programma te kunnen lopen worden netjes bijgehouden en voor de release weer allemaal verwijderd. In een MMORPG zijn dus meestal geen codes terug te vinden omdat ze nooit ingebouwd zijn of allemaal netjes zijn verwijderd. Mocht toch blijken dat er eentje is achtergebleven dan kan dat simpel opgelost worden door een verplichte patch uit te brengen.

Dan het cheaten via user interfaces. Hiervan is al eerder aangegeven dat dit een vrij grijs gebied is. Binnen de meeste MMORPGs is het aanpassen van de UI een verschijnsel dat door zowel de fabrikant als de community geaccepteerd is. Gemodificeerde UI's tonen bijvoorbeeld extra informatie over tegenstanders, berekenen hoeveel schade er precies gedaan, bieden extra knoppen, enzovoorts. Waarschijnlijk wordt dit niet als cheaten gezien omdat de gemodificeerde UI's door iedereen te downloaden zijn en dat het algemeen bekend is dat ze gebruikt worden. Iemand die zich benadeeld voelt omdat iemand anders er gebruik van maakt kan dus eenvoudig dezelfde mod downloaden om zo hetzelfde voordeel te behalen. Gamers die niet zitten te wachten op bergen extra info op het scherm laten deze mods simpelweg achterwege en vinden dat niks toevoegen aan de game. Het is dus meer een kwestie van voorkeur dan een kwestie van cheaten.

Links een standaard interface, rechts een gemodificeerde interface.

4.3. De anti cheatmethodes

Fabrikanten laten cheaters natuurlijk niet zomaar hun gang gaan, ze doen er veel aan om ze tegen te werken. Hier gebruiken ze verschillende methodes voor die verder uitgewerkt en beschreven zullen worden. Er wordt eerst een korte geschiedenis gegeven van de online games en de achterliggende architectuur. Aangezien het de bedoeling is om de methodes te beoordelen op hun sterke en zwakke punten is er een lijst met criteria opgesteld waarop de methodes beoordeeld zullen worden. Deze lijst is terug te vinden in 4.3.3. Hierna worden de methodes apart beschreven en wordt er aangegeven welke cheats ermee tegen worden gewerkt. Aan de hand van de manier waarop de methode met die cheats omgaat kunnen de aspecten per methode geanalyseerd worden.

4.3.1. Een korte geschiedenis

De netwerkarchitectuur die een game gebruikt bepaalt grotendeels hoe gevoelig deze is voor cheaters (ArenaNet, 2006). Het meest gevoelig voor cheaten is een a-synchrone peer-to-peer-connectie. Deze verbinding is het beste te vergelijken met een telefoongesprek. De ontvangende kant kan de correctheid van de ontvangen data meestal niet verifiëren. Bij deze connectie is het vrij makkelijk om verstuurde data aan te passen zonder dat de ontvangende kant ook maar iets doorheeft. Tegenwoordig komt het bijna niet meer voor, maar het werkt op deze wijze: speler A komt speler B tegen op het slagveld. Speler A raakt speler B voor 20 punten. Het gegeven dat speler B geraakt is voor 20 punten is bekend aan de kant van speler A, maar moet nog naar speler B gestuurd worden om te zorgen dat de twee computers gesynchroniseerd blijven. Als de waarde 20 voor verzending veranderd wordt naar 40, ontvangt speler B alleen deze waarde en is het voor hem onmogelijk om te ontdekken dat er vals gespeeld wordt. Een bekend praktijkvoorbeeld hiervan is te vinden in de online game Diablo. Alle spelers beginnen in hetzelfde dorpje dat dienst doet als ‘safety zone’. In deze zone kunnen spelers elkaar niet aanvallen. Toch vonden cheaters een manier om andere spelers te raken, ze verzonden simpelweg een bericht met: ik raak jou voor 20 punten. Andere computers accepteerden dit bericht zonder morren en trekken 20 health points van hun speler af.

Een eerste poging om dit probleem op te lossen was de synchrone peer-to-peer connectie. Hierbij bevinden alle partijen zich op precies hetzelfde punt in de game. Gevolg hiervan is wel dat er zogenaamde lag optreedt: de snellere speler kan niet verder voordat de tragere alle informatie verwerkt heeft.Daarnaast wordt bij synchrone peer-to-peer connectie in de meeste gevallen alleen informatie over ingedrukte toetsen en muisklikken over gestuurd. In plaats van “ik raak jou voor twintig punten” wordt de boodschap: “ik klik op jouw bovenbeen”, waarna de ontvangende kant zelf de schade kan berekenen. Toch blijft deze methode erg gevoelig voor cheaters omdat iedere computer alles moet weten over iedere speler om het spel te kunnen draaien. Via cheaten is het dan bijvoorbeeld nog mogelijk om de positie van de tegenstander te achterhalen of om te weten met welk wapen hij rondloopt.

Het probleem bestond er dus voornamelijk uit dat cheaters informatie konden veranderen en informatie konden bekijken die alleen bedoeld was voor de tegenpartij. Er werd weer een nieuwe netwerkarchitectuur ontworpen voor multiplayer games: het client-server model. In dit model stuurt iedere client alle benodigde informatie naar een server. Deze server verwerkt alle informatie over de spelomgeving en past deze aan naar de acties van de clients. Vervolgens stuurt de server naar iedere client alleen die informatie die deze nodig heeft. Hierdoor kan een cheater geen data meer bekijken die hij niet onder ogen mag krijgen en door het controleren van de verzonden informatie voorkomt de server (grotendeels) dat deze aangepast wordt.

Maar hoe weet de client dat de server te vertrouwen is? Dat is vrij simpel: niet. De server heeft erg veel macht over de game en de beheerder kan op allerlei manieren cheaten. Hoewel erg vervelend is dit geen groot probleem in games waarbij gewerkt wordt met korte potjes. Een gemiddeld potje Counter Strike duurt een paar minuten. Blijkt tijdens die potjes dat de server niet te vertrouwen is dan wordt deze geboycot en wordt er een andere gezocht. Moeilijker wordt het in MMORPGs. Hier worden geen korte potjes gespeeld maar worden honderden uren gestoken in een enkel karakter. De server draait continu en iedere speelsessie ontwikkelt een karakter zich verder. Het is duidelijk dat een onbetrouwbare server hier wel heel veel schade kan aanrichten, aangezien het meestal niet mogelijk is het karakter over te brengen naar een andere server. Daarom wordt er bij de meeste MMORPGs gewerkt met hosted environments. Dit betekent dat de producent van de game zelf de servers draait en dat enkel op deze servers de game te spelen is. Hierdoor houden ze zelf het overzicht en kan alle informatie geanalyseerd worden. Voor de gamers levert het zekerheid omdat ze meer vertrouwen in de producent kunnen hebben dan in een willekeurige gamer die een server gestart heeft. De eerste moet er namelijk zijn brood mee verdienen en heeft een naam die op het spel staat, de tweede is veelal anoniem en zal niet vaak een reputatie hebben die beschadigd kan worden.

4.3.2. Het contract tussen gamer en fabrikant

Als is geconstateerd dat iemand zich niet aan de regels houdt, wat kan de producent dan doen? Voordat je als gamer toegang krijgt tot de spelwereld moet de gekochte game geregistreerd worden bij de fabrikant. Op dat moment moet er een gebruikersovereenkomst/policy geaccepteerd worden waarin staat wat er precies verboden is (WoW, 2006). Er staat ook in dat de producent in het geval van het breken van de overeenkomst door de gebruiker actie mag ondernemen. Deze actie bestaat meestal uit het ontzeggen van de toegang tot de servers, het zogenaamde bannen. Gamers waarvan bekend is dat ze cheaten hebben worden op deze manier geweerd uit de game zodat de anderen ongestoord kunnen gamen. Omdat zowel de game (door patches) zelf als de manier waarop gecheat wordt constant veranderen wordt deze policy regelmatig ge-update waarna deze weer opnieuw door de gebruiker ondertekend moet worden zodat de fabrikant in zijn recht blijft staan. Bannen is namelijk alleen mogelijk als iemand de expliciete regels heeft overtreden.

4.3.3. Op welke wijze kunnen methodes beoordeeld worden?

Op basis van ervaring met traditionele software en MMORPGs heb ik een lijst opgesteld met criteria die gebruikt kunnen worden om anti-cheatmethodes te kunnen beoordelen. Met deze criteria zijn de belangrijkste kenmerken van de methodes gedekt. Voor iedere methode worden in het volgende onderdeel de criteria ingevuld zodat de methodes beoordeeld kunnen worden. Deze beoordeling is vrij simplistisch. Dit wordt veroorzaakt door het karakter van dit onderzoeksgebied. Er is weinig bekend over waar goede anti-cheatmethodes aan moeten voldoen en er is ook weinig bekend over in hoeverre hieraan voldaan wordt. In het achterhoofd moet dan ook gehouden worden dat nergens wordt beweerd dat dit dé beste methode is. Voor de score wordt gebruikt maakt van een beoordelingschaal bestaande uit: **+**, **0** en **-**. Dit is een vrij ruwe schaalverdeling die gebruikt wordt omdat er geen precieze informatie bestaat over dit onderwerp. Wel kan ingeschat worden of een methode goed, gemiddeld of slecht scoort op een bepaald onderdeel. Hóe goed of slecht het is is in principe niet relevant: het gaat in deze scriptie vooral om de sterke en zwakke plekken, niet om precies in te schatten hoe sterk of hoe zwak deze dan zijn.

De lijst met criteria waarop de methodes beoordeeld worden:

- **Privacy:** wat is de invloed van de methode op de privacy? Hoe goed worden de gegevens van de gebruiker beschermd, wat wordt onderzocht en wat niet? Is het wel legaal om op deze manier cheaters op te sporen?

- **Effectiviteit:** hoe effectief is de methode in het bestrijden van de specifieke cheat? Worden alle mogelijkheden afgevangen of blijven er gaten bestaan?

- **Gebruik van resources:** Hoeveel bandbreedte kost het om de methode te gebruiken, hoeveel servercapaciteit of processorkracht kost het om een methode te gebruiken?

- **Kosten:** Hoe duur is het om een methode te ontwikkelen of te gebruiken? Zijn dit eenmalige kosten of kosten die gedurende de hele looptijd blijven ontstaan?

4.4. De beoordeling van de methodes

In dit onderdeel worden zoals eerder vermeld verschillende bekende methodes die men gebruikt om cheaten tegen te gaan besproken. Per methode wordt vervolgens aangegeven welke vormen van cheaten erdoor worden aangepakt en in welke mate hij aan de opgestelde criteria voldoet.

4.4.1. Het client-server model

Het eerder beschreven client-server model past goed bij een gouden regel in de online gaming industrie: don't trust the client. In de praktijk betekent dit dat zoveel mogelijk informatie op de server blijft en zo min mogelijk naar de client gestuurd wordt. In principe kun je een online game op twee manieren draaien:

- Alle informatie wordt op de computer van de client verwerkt. Naar de server wordt informatie gestuurd over hoe de gebruiker de wereld heeft beïnvloed. Deze informatie wordt door de server doorgestuurd naar de andere clients die het weer gebruiken om hun gamewereld te updaten.

- Alle informatie wordt op de server verwerkt. Daarna wordt de verwerkte informatie naar de clients gestuurd. Denk hierbij aan informatie over wat de speler ziet, welke monsters er in beeld zijn of wat de status van het karakter is. De enige informatie die de client terugstuurt is welke acties hij maakt. De server berekent de invloed van die acties op de gamewereld en past deze weer aan.

De eerste methode kost weinig bandbreedte en servercapaciteit: er wordt weinig informatie van de server naar de client gestuurd en er is weinig informatie die door de server verwerkt moet worden omdat dit door de client wordt gedaan. De tweede methode kost meer bandbreedte en servercapaciteit: veel informatie over de spelwereld moet naar de client gestuurd worden zodat deze de wereld kan tonen aan de gebruiker. De veranderingen van de spelwereld die teweeg worden gebracht door de gebruikers worden berekend door de server. Hoewel de tweede methode een stuk minder gunstig lijkt is dit wel de basismethode waarvan uit wordt gegaan door producenten. Hoe meer informatie door de server berekend wordt, hoe minder informatie door de gebruiker bewerkt kan worden. Als de gebruiker weinig kan veranderen aan de informatie wordt de mogelijkheid tot cheaten verkleind. Het nadeel hiervan is de gebruikte bandbreedte: als er veel informatie verzonden moet worden dan neemt de lag toe, er moet dus naar een goede balans gezocht worden tussen veiligheid en snelheid.

Effectgebied

Het gebruik van het client-server model en het 'don't-trust-the-client'-principe vangt twee cheatproblemen af:

- De uitrusting: cheaten via de connectie. Door stabiele software wordt voorkomen dat er items gedupliceerd worden door de software te laten crashen.

- De interactie: cheaten via de connectie. Doordat de client alleen die data krijgt die hij nodig heeft en de teruggestuurde data steeds geverifieerd wordt is het erg moeilijk om de data aan te passen en op deze manier te cheaten. Iedere handeling wordt gemonitord zodat verdachte data onderschept wordt.

Beoordeling

- **Privacy** **+** Het voorkomen van cheaten via het client-server model doet geen afbraak aan de bescherming van de user, het draagt er zelfs aan bij. Doordat alle communicatie via de server verloopt is bijvoorbeeld het IP-adres van de gebruiker alleen bij de server bekend.

- **Effectiviteit** **+** door de invoering van het client-server model is het cheaten door data aan te passen zo goed als uitgestorven. Omdat de server alle data analyseert valt iedere afwijking op en worden cheaters snel gedetecteerd.

- **Gebruik van resources** **+** Zoveel mogelijk informatie wordt verrekend en verwerkt op de server . Hoewel de server dus veel rekenwerk heeft wordt hierdoor wel de client ontzien. De gebruikte server heeft deze capaciteit toch al, terwijl het per client verschilt of zijn beschikbare hardware hier goed genoeg voor is. Dit gecombineerd met het feit dat alleen de benodigde informatie tussen de client en de server verstuurd wordt zorgt ervoor dat het client-server model efficiënt gebruik maakt van de beschikbare resources.

- **Kosten** **+** Als vanaf het begin van de ontwikkeling er rekening mee gehouden wordt dat deze netwerkarchitectuur gebruikt gaat worden, ondersteund door dit principe, dan hoeft het geen extra kosten met zich mee te brengen. Wat wel duur is, is het aanpassen van eenmaal bestaande games naar een fundamenteel ander netwerkmodel, dit is dan ook iets wat dan ook bijna niet voorkomt.

4.4.2. Moderators

In de spelwereld zelf wordt gecontroleerd door moderators. Moderators zijn mensen die als karakter rond lopen in de wereld. Gamers met problemen kunnen bij hen terecht en zij zoeken dan naar een oplossing. Ze hebben veel meer rechten dan een standaard gebruiker. Zo kunnen ze items creëren en laten verdwijnen, ze kunnen gamers verplaatsen, enzovoorts. Naast het helpen van gamers met problemen vervullen ze ook de rol van politieagent. Zo letten ze ook op of er ergens gecheat wordt, of er ongepast gedrag vertoont wordt en of er gamers met ongewenste namen rondlopen. Om de boel in de gaten te houden maken ze veel gebruik van andere gamers die rondlopen en gedupeerd zijn door een cheater. Deze gedupeerden melden maar al te graag wie hen opgelicht heeft waarna de moderator actie kan ondernemen.

Effectgebied

- De uitrusting: oplichting. Moderators kunnen ingezet worden om oplichters op te sporen. Users die zijn opgelicht kunnen naar een moderator toestappen en hun beklag erbij doen. Het blijft natuurlijk moeilijk om daarna achter de echte waarheid te komen, er zijn altijd twee kanten van een verhaal. Naarmate een oplichter meerdere gebruikers oplicht wordt het echter gemakkelijker om hem/haar te achterhalen.

- De eigenschappen van het karakter: externe software. Cheaters die een programma gebruiken dat automatisch zorgt dat de speler beter wordt zijn te herkennen aan het voorgeprogrammeerde gedrag dat een gebruiker vertoond. Het karakter handelt namelijk volgens een vast patroon wanneer deze bestuurd wordt door een programma. Een moderator kan dit gedrag signaleren (of iemand anders wijst de moderator erop) en kan dan actie ondernemen.

Beoordeling

- **Privacy 0** Moderators kunnen meer informatie over een gebruiker opvragen als ze vermoeden dat deze cheat. Hoe vaak dit gebeurt en wat ze dan analyseren is niet bekend omdat dit gevoelige informatie is. Het is echter geen gekke gedachte dat historische gegevens over het spelgedrag van gebruikers nagetrokken worden op het moment dat er vermoed wordt dat deze cheat.

- **Effectiviteit** – De effectiviteit wordt bepaald door de hoeveelheid moderators en hun prioriteiten. Precieze informatie over hoeveel tijd moderators besteden aan het opsporen van cheaters is niet bekend, maar de gedachte is dat hier niet heel veel tijd aan besteed wordt. Met duizenden gebruikers zijn ze vooral bezig met het helpen van gebruikers die directe problemen hebben waardoor hun spelplezier afneemt

- **Gebruik van resources** + het inzetten van moderators kost bijna niks aan extra resources. Natuurlijk lopen ook zij rond in de wereld en moet de server hier rekenkracht aan besteden, maar aangezien er nog duizenden anderen rondlopen valt dit in verhouding mee.

- **Kosten –** Moderators zijn zeker in de grote MMORPGs geen vrijwilligers en zullen dus betaald moeten worden. De kosten van moderators zijn evenredig met het aantal en het aantal uren dat ze ingezet worden. Deze kosten blijven bestaan zolang er moderators ingezet worden, wat meestal gelijkloopt met de levensduur van de game. Het inzetten van moderators is dus zeker in vergelijking met de andere methodes een kostbare keuze. Aangezien ze niet alleen ingezet worden om cheaters op te sporen maar een veel bredere taak hebben valt de keuze toch te verantwoorden.

4.4.3. Externe programma's

Externe programma's draaien buiten de hoofdapplicatie (de game) om. Hier wordt nog vrij weinig gebruik van gemaakt. Externe programma's worden vooral gebruikt om externe cheatprogramma's op te sporen. Blizzard, de maker van de populaire MMORPG World of Warcraft maakt gebruik van zo'n extern programma om cheaters op te sporen. Een klein programma genaamd 'de Warden client' wordt geïnstalleerd om de computer van de cliënt en verzamelt terwijl WoW draait informatie over andere programma's die draaien op de computer van de gamers, en stuurt deze in bepaalde situaties terug naar Blizzard. Dit programma dient als voorbeeld van een extern programma dat als anti-cheatmethode wordt ingezet. Omdat er (volgens mijn kennis) geen andere externe methode is die hier op lijkt wordt de Warden als hét externe programma beschouwd, de uiteindelijke beoordeling is dan ook specifiek gericht op de Warden en niet op externe programma's in zijn algemeenheid. De onderstaande beschrijving komt rechtstreeks van de website FOK!games en is ook door mij geschreven (FOK!, 2005).

De Warden wordt ongeveer iedere vijftien seconden uitgevoerd en verzamelt dan drie soorten informatie: ten eerste verzamelt hij alle DLL's die aangeroepen worden wanneer World of Warcraft wordt gestart. Een DLL is een bibliotheek met functies die door meerdere applicaties aangeroepen kan worden. Hiermee wordt voorkomen dat een functie die door meerdere programma's gebruikt wordt onnodig meerdere malen draait. Dat de Warden deze controleert is niet zo erg, DLL's zijn openbaar en op iedere (Windows)PC te vinden. Als bekend is welke DLL's iemand gebruikt dan weet je niet iets echt spannends. Blizzard controleert dit om er zeker van te zijn dat op dit gebied niet geknoeid wordt om te kunnen cheaten.

Het tweede proces is het scannen van de tekst in de titel van ieder venster dat je open hebt staan. Hierbij wordt geen onderscheid gemaakt tussen vensters die openstaan om WoW te kunnen spelen (zoals het venster waar WoW zelf in draait) en andere vensters. Heb je bijvoorbeeld de index van FOK!games geopend in FireFox dan is deze tekst "FOK!games – index – Mozilla FireFox". Hierdoor wordt niet alleen informatie verzameld over welke webpagina's je bezoekt, maar bijvoorbeeld ook over met wie je spreekt op msn, in welke kanalen van IRC je je begeeft en wat hier het wachtwoord van is, aan welke documenten je werkt, enzovoorts. Vervolgens worden deze titels gehashed (kort door de bocht is 'hashen' een simpele vorm van het coderen van tekst) en vergeleken met een lijst van 'banning hashes'. Is een van de gegenereerde hashes gelijk aan een van deze banning hashes dan weet de Warden dat je gebruik maakt van cheatprogramma's. Is er een banning hash gedetecteerd dan wordt dit doorgegeven aan Blizzard en dan kunnen zij actie ondernemen.

Als laatste kijkt de Warden naar het ‘process memory’. Wat hier valt te zien zijn alle processen die je hebt draaien. De interessante stukken in het geheugen worden uitgelezen en ook weer gehashed en met de lijst van ‘banning hashes’ vergeleken. Deze checks worden gedaan om te detecteren welke andere programma’s je op de achtergrond hebt draaien. Interessant voor Blizzard zijn cheatprogramma’s als WoWglider. Om erachter te komen welke cheatprogramma’s er nu precies draaien, zullen alle programma's bekeken moeten worden. Zo worden bijvoorbeeld alle programma's die rechtsonder in je taakbalk staan gechecked maar ook alle andere programma's die draaien maar die daarvoor geen venster hebben openstaan.

Het hashen van de stukjes tekst en het vergelijken met de lijst van banning hashes gebeurt allemaal op de computer van de gebruiker. Komt er een hash uitgerold die wijst op het gebruik van ongewenste software dan wordt dit doorgegeven aan Blizzard. Er wordt dus alleen actie ondernomen als er daadwerkelijk een ongeoorloofd programma is gedetecteerd en alleen het gegeven dat dat programma is gedetecteerd wordt doorgegeven. Informatie over andere programma's of hashes hiervan wordt dus niet teruggestuurd naar de servers van Blizzard. (Rootkit, 2005)

Effectgebied

- De eigenschappen van het karakter: externe software en de interactie: externe software. Omdat de Warden onderzoekt wat er buiten de game omdraait aan programma’s is deze effectief in het opsporen van externe software die wordt gebruikt om de eigenschappen van het karakter te verbeteren of om de interactie te beïnvloeden. Hij houdt precies in de gaten welke andere programma’s ernaast gedraaid worden en heeft dus meteen door wanneer er gebruik gemaakt wordt van cheatprogramma’s. Tenminste, zolang de cheatprogramma’s zelf niet aangepast worden om de Warden weer te omzeilen. Het blijft natuurlijk een kat-en-muis-spel.

Beoordeling

- **Privacy –** Het installeren van software op de computer van de client zonder dat deze daar expliciet over ingelicht is om daarna zijn/haar draaiende processen te kunnen monitoren is nogal een inbreuk op de privacy. In de voorwaarden die ondertekend moeten worden voordat er gebruik kan worden gemaakt van World of Warcaft staat wel een alinea over de Warden. Het is nogal optimistisch om ervan uit te gaan dat iedereen dit leest en er bewust mee instemt dat dit soort software mee geïnstalleerd wordt met de game. Officieel is het niet verboden om dit soort programma's mee te leveren maar dat wordt meer veroorzaakt door het ontbreken van fatsoenlijke privacywetgeving ter bescherming van het individu op internet dan doordat er echt over nagedacht is. Doordat dit soort games wereldwijd gespeeld wordt is het zeer moeilijk om er een wet voor te maken die precies bepaald wat wel en wat niet geoorloofd is. Tot die tijd hebben fabrikanten veel speelruimte, ook op gebieden waar deze ruimte erg discutabel is.

- **Effectiviteit +** Het is een effectieve manier om externe programma's op te sporen aangezien direct gemonitord wordt wat er nog meer draait aan programma's. Draaien er cheatprogramma's dan wordt deze ook direct ontdekt.

- **Gebruik van resources 0** Een extern proces zal enige processorkracht opeisen maar de berekeningen die erdoor uitgevoerd worden zijn vrij klein. Ook wordt af en toe de verbinding gebruikt om data te versturen. Omdat er toch data verwerkt wordt en er bandbreedte gebruikt wordt staat hier een 0.

- **Kosten +** Ook hiervoor geldt dat als het programma eenmaal ontwikkeld is er geen verdere kosten meer aan verbonden zijn. Na de release wordt het programma mee geïnstalleerd op iedere gebruikerscomputer en verzamelt en verwerkt vervolgens alle informatie automatisch, waardoor er bijna geen extra kosten aan het gebruik verbonden zijn.

6.Conclusie

De analyse van de methodes op hun sterke en zwakke punten kan samengevat worden in een tabel:

	Privacy	Effectiviteit	Gebruik van resources	Kosten
Client-server model	+	+	+	+
Moderators	0	–	+	–
Externe programma's	–	+	0	+

Een zwak punt van de huidige methodes blijft het opsporen van oplichters. Dit wordt ook veroorzaakt doordat vaag is wat nu precies oplichting is: is het oplichting als iemand op een slimme manier handel bedrijft en producten beter laat lijken dan ze zijn daar halve waarheden te vertellen, of is het pas oplichting als hij daadwerkelijk liegt over zijn handelswaar? Voor mensen is het al moeilijk om dit in te schatten, laat staan door computers. Het is moeilijk om automatisch oplichters op te sporen, daarom worden daar nu nog vooral mensen voor ingezet. Dit is erg duur is en niet zo effectief door de vele aspecten die hierin meespelen.

Een ander zwak punt is hoe cheaten met behulp van externe programma's wordt opgespoord. Doordat hier momenteel een extra programma voor geïnstalleerd wordt waarvan de gebruiker niet helemaal correct van op de hoogte wordt gesteld wringt deze methode op het gebied van privacy en legaliteit. De gebruiker verliest de macht over zijn computer en weet niet meer wat er allemaal op geïnstalleerd staat. Daarnaast wordt er informatie over het gebruik van zijn computer verzameld en (weliswaar versleuteld door middel van hashing) teruggestuurd naar de fabrikant. Heeft deze daartoe wel het recht? Dit is nog een erg schimmig gebied en het blijkt weer eens dat de rechtstaat achter de feiten aanloopt en de huidige snelle ontwikkelingen niet bij kan benen.

Een sterk punt van de huidige methodes is dat het erg moeilijk is om met de data zelf te knoeien. Doordat het meeste door de server zelf berekend wordt en alle data geanalyseerd wordt is het erg moeilijk om nog op deze manier te cheaten. Cheat codes zitten niet in MMORPGs omdat deze niet ingebouwd worden of voor de release weer verwijderd worden. Het aanpassen van user interfaces is een algemeen geaccepteerde manier om de game aan te passen dus dat vormt ook geen probleem, ook al verschaft het de ene gebruiker een voordeel ten opzichte van de andere.

Wat nu duidelijk is, is waar de zwakke plekken liggen in de huidige methodes om cheaten tegen te gaan. Oplichters vormen een groot probleem, en ook het beschermen van de privacy van de user is een belangrijk punt. Hoe hier dan wel mee omgegaan zou moeten worden en wat dan wél een goede oplossing is, is iets wat nog verder onderzocht kan worden. Het is in ieder geval belangrijk dát er dieper op ingegaan wordt, omdat de markt explosief groeit en de belangen toenemen. Het is onacceptabel als er lukraak methodes ontwikkeld worden die bepaalde problemen niet aanpakken of in hun aanpak rechten schenden. Deze ontwikkelingen worden gelukkig kritisch in de gaten gehouden door de gamers zelf, maar het is van belang dat ook de academische wereld en de overheid erbij betrokken raken om te voorkomen dat grote bedrijven doen waar ze zin in hebben in hun jacht naar het grote geld. Dat bedrijven vrij ver gaan in hun jacht op geld is wel duidelijk, er moet tegenwicht geboden worden om de rechten van de gebruiker te beschermen.

Het zou beter zijn als al voor de aanschaf van een product duidelijk is dat programma's zoals de Warden geinstalleerd worden; het kan bijvoorbeeld op de doos vermeld worden. Daarnaast zou het netjes zijn als de broncode van de Warden wordt vrijgegeven zodat iedereen voor zichzelf kan controleren wat er nu precies gebeurt, wat er verzameld wordt en hoe hier mee omgegaan wordt. Hierdoor wordt dit programma wel weer een stukje kwetsbaarder voor concurrentie en cheaters. Als de vergelijking wordt gemaakt met encryptiealgoritmes lijkt dit toch een vrij logische stap. In de wereld van de encryptie is het namelijk gebruikelijk dat het encryptiealgoritme bij iedereen bekend is en dat de kracht van het algoritme bij het gebruik van de sleutels ligt (Tanenbaum, 1996). Dat concurrenten hierdoor een voordeel krijgen is misschien een offer dat gebracht moet worden om de privacy van de gebruikers enigszins te blijven respecteren.

7. Reflectie & referenties

Qua literatuur zijn cheaten en MMORPGs geen onderwerpen waar veel informatie over te vinden is. Gamen is zeker in vergelijking met andere vormen van tijdverdrijf erg jong en veel onderzoek is er dus nog niet naar gedaan. Voor de achtergrond van hoe de methodes beschreven en beoordeeld kunnen worden heb ik veel gehad aan het boek *Software Quality Assurance : From Theory to Implementation* van Daniel Galin. Een gezond niveau van paranoïde ten opzichte van software en security heb ik ontwikkeld door een tweetal boeken op het gebied van software security: *IT Governance; A Managers Guide To Data Security And BS7799/ISO17799* van Alan Calder en Steve Watkins en *Computer Networks* van Andrew S. Tanenbaum.

Moeilijker is het om precies de bronnen van mijn kennis over MMORPGs, cheating en gaming aan te duiden. Ik game al relatief lang en heb een tijd intensief deelgenomen aan de MMORPG World of Warcraft. Mijn interesses reiken verder dan alleen het spelen van games, daarom ben ik me meer en meer gaan verdiepen in de achtergrond ervan. Zo kwam ik terecht op forums als http://forum.fok.nl/ (Nederlandse community), http://www.igda.org/Forums/ (community van game developers, onderzoekers, studenten en andere geïnteresseerden) en het forum van de World of Warcraft community: http://forums-en.wow-europe.com/. Hierdoor heb ik mijn kennis kunnen verbreden en heb ik veel geleerd over de achtergronden van gaming. Ik vervul momenteel ook de functie van eindredacteur bij het specifieke gamesgedeelte van jongerenwebsite FOK!: http://games.fok.nl/. Van daaruit heb ik de mogelijkheid gehad om naar de grootste internationale conferentie op gamegebied te gaan: de E3 in Los Angeles (http://www.e3expo.com/). Hier heb ik ervaring opgedaan door het volgen van specifieke work shops op het gebied van MMORPGs. Hoewel mijn bronnen voor deze scriptie voornamelijk niet wetenschappelijk zijn (Wikipedia en andere websites) kan ik op grond van mijn ervaring goed inschatten in hoe betrouwbaar deze bronnen zijn.

Voor het onderzoek heb ik ook geprobeerd om MMORPG-fabrikanten te benaderen en ze te vragen mee te helpen aan dit onderzoek. Achteraf bleek dit vrij naïef want geen enkele bleek bereid om terug te mailen, laat staan mee te helpen aan het onderzoek. Dit wordt mede veroorzaakt door de slechte bereikbaarheid (mailen naar de supportafdeling om te vragen of ze mee willen helpen aan een onderzoek is nu eenmaal niet zo'n goede manier om 'binnen te dringen') en de aard van het onderwerp. Cheaten en de methodes hiertegen hebben direct invloed op de core business van deze bedrijven. Het was achteraf gezien dus te verwachten dat ze hierover niet loslippig zouden zijn richting onderzoekers. Gelukkig kon ik deze scriptie toch schrijven op basis van de informatie die op internet gevonden kon worden, maar het had zeker toegevoegde waarde gehad als fabrikanten bereidwilliger waren geweest om mee te werken.

8. Bronvermelding

(Wordnet, 2006) Wordnet, Princeton University Cognitive Science Laboratory http://wordnet.princeton.edu/, Juni 2006

(Wikipedia, 2006) Wikipedia, the free Encyclopedia, online games, http://en.wikipedia.org/wiki/Online_game, Juni, 2006

(Wikipedia, 2006) Wikipedia, the free Encyclopedia, Adventure http://en.wikipedia.org/wiki/Adventure_%28Atari_2600%29, Juni 2006

(Wikipedia, 2006) Wikipedia, the free Encyclopedia, Cheat codes http://en.wikipedia.org/wiki/Cheat_code, Juni 2006

(Wikipedia, 2006) Wikipedia, the free Encyclopedia, Cheating in online games http://en.wikipedia.org/wiki/Cheating_in_online_games, Juni 2006

(ArenaNet, 2006) Mike O'Brien & Gaile Gray, Game Cheats and Cheat Prevention http://www.arena.net/news/articles/mikearticle040802.html, Juni, 2006

(WoW, 2006) World of Warcraft, User Policy http://faq.wow-europe.com/en/policy/, Juni, 2006

(FOK!, 2006) FOK!games, Alex Hamakers, World of Spycraft? Big Blizzard is watching you! http://games.fok.nl/review.php?reviewid=8045, December 2005

(rootkit, 2005) Rootkit, Greg Hoglund http://www.rootkit.com/blog.php?newsid=358

(Tanenbaum, 1996) *Computer Networks*, Andrew S. Tanenbaum, 1996

Literatuur:

Tanenbaum, Andrew S, *Computer Networks*, Prentice Hall PTR, 1996

Galin, Daniel, *Software Quality Assurance : From Theory to Implementation,* Addison Wesley, 2003

Calder, Alan, Watkins, Steven IT Governance; A Managers Guide To Data Security And BS7799/ISO17799, Kogan Page 2005