NTNU
Det skapende universitet

Brukersikkerhet i spillindustrien

Jarle Lindseth

Master i kommunikasjonsteknologi
Oppgaven levert: Juli 2010
Hovedveileder: Øivind Kure, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Kartlegge og analysere brukersikkerhetsrutiner i spillindustrien

Oppgaven gitt: 28. februar 2010
Hovedveileder: Øivind Kure, ITEM

User Authentication in Online Gaming

TTM4900 - Mastgeroppgave

by

Jarle Lindseth

July 25, 2010

Veileder:
Prof. Øyvind Kure
....

Norges Teknisk-Naturvitenskapelige Universitet

Fakultet for informasjonsteknologi, matematikk og elektroteknikk

Institutt for telematikk

Project Assignment

Student's name: Jarle Lindseth

Course: TTM4900 Master Thesis

Title: User Authentication in Online Gaming.

Description (composed by the student):

This assignement will attempt to map some of the various threats and challenges the online gaming industry face in the field of user authentication and account security. Specifically in regards to what seperates it from other industries.

It will examin the various solutions, currently available and theoretically possible, that the gaming industry might use to solve this security problem. It will do this in regard to technological possibility, financial cost and social useability. Finally it will try to present a recommendation that is implementable, acceptable to users and financially feasible.

Deadline: July 25th, 2010

Submission date:

Department: **Department of Telematics**

Supervisors: **Øyvind Kure, NTNU**

Øyvind Kure **Date**

Preface

This paper is the result of a long personal interest in the field of both online gaming and information security. Its inception came about in two parts and it lay dorment for a long period of time before starting my master thesis. My own observations of the rampant account-compromises across several gaming titles together with an inherent skepticism of needing to carry a dedicated physical authentication chip for such services as banking web sites led to a lot of frustration.

While a long-time favourite of mine was allways the solution of transmitting a one-time code via SMS to a mobile phone I had a feeling that such a solution would not be apropriate to adopt for game developers. This lead me to the realisation that I could propose developing an application for mobile phones that could take on the role of the authentication code generator as my masters thesis.

When I read in a press release that another company released just such a device I felt both pride and dissapointment, and for a long time the entire idea was abandoned and forgotten.

As it became time for me to start my master's thesis it dawned on me that there still was a lot of unsolved issues with the account security of online gaming and at about this time the first proven incident where game accounts using authenticators had been compromised surfaced.

It is my belief that the specificality of the issues seperating the online gaming industry from comparable industries has not been satisfactorily examined before, and to the best of my knowledge the descriptions and recommendations in this paper are original. In the cases where no citations or references are made to systems I describe the ideas are my own.

However big of a market online gaming is, it is not widely studied in academic circles and if any contemporary works on the same subject exists it is purely coincidental.

Contents

Abstract

This paper has been divided into several parts. Each part assuming knowledge of the issues discussed in the previous parts, but not necessarily being a continuation of that part. It begins with an introduction to online gaming, a brief history of its evolution and some insight into how the ingame economies work. As well as some discussion of how the virtual ingame values relate to real world values and how that complex relationship causes problematic incidents.

A brief summary of the motives, methods of attack and the threat level of the industry is given as well as a comparative analysis of related industries; which ways the online gaming industry is similar to them and in which ways it differs. This gives an idea of what can be learned from more mature or developed industries and in which areas the gaming industry needs to find its own way and develop its own standards.

Building on these similarities and differences a variety of additional security options are discussed. Their respective strengths and weaknesses in relation to both the comparative industries and the gaming industry itself are mentioned. Specific security incidents as well as general trends in the field are explained and used to substantiate some claims to recent and future developments.

Finally, the conclusion summarizes the key points from the previous chapters and attempts to make an assessment of how a game developer should go about deciding on a security scheme as well as a prediction on how security in the gaming industry will evolve over the next few years.

Scope of Security

This paper analyses account security in the case of online gaming. The Focus is on whether or not anyone will be able to gain unlawful access to an account and its contents.

While establishing confidentiality is a normal practice it is not the focus of this paper. Gaming is, primarily, a recreational activity and the information in these systems can be regarded as not being sensitive. Therefore tools used to log and reverse acts performed by wrongly authenticated persons are discussed as an alternative to having a strong authentication.

Methodology

Knowing what methodology to adopt when working on a problem is important as it allows imcreased awareness of the potential strengths and weaknesses of the chosen methodology. In any scientific work objectivity is paramount, and in that regard it is essential to be aware of the approach used in order to prevent unnecessary bias.

Much of the cases and findings represented in this paper have a basis in my own experiences and those gleaned from associates over time. These are definitely coloured by individual opinions and one-sided accounts. Keeping this in mind I have attempted in all possible situations to acquire second and third perspective on the subject and tried to verify all data through secondary sources.

As a means to gather opinions on several topics outside of those available publicly I have conducted a set of interview with a group of players from the game World of Warcaft, these interviews were conducted online through email, instant messaging and forums depending on the preferrence of the subjects. Answers were in part quantitative in those cases where they were simple yes-or-no-questions or questions concerning amounts; and in part qulitative in those cases that I asked them about their own opinions on the scale of a given problem, their preference of a solution or other personal experiences. A total of fifty different people were questioned. The results have been used as necessary background information and inspiration for this paper, but their answers have also been used directly in the paper in several places.

A large portion of the paper is dedicated to describing the evolution of events and important incidents. These were researched in news reports and first-hand user descriptions from a wide variety of sources and I have attempted to allways collect additional sources for each. The ones cited in this paper were the most credible and the most exhaustive of the them.

Articles from Wikipedia have been used as general background research, but all data has been verified externally and completely. The citations in this paper to articles on Wikipedia are only meant as recommended reading for those without prior understanding of the terms or items in question on subjects that are related to, but outside the scope of this paper.

1 Online Gaming

This part of the paper is intended to give the reader a basic knowledge of online gaming industry, including its history and the way it has evolved in the last two decades.

Furthermore it attempts to describe some of the emergent systems in the games and the way that these extend over to the real world. In particular the complex relationship between ingame virtual possessions and actual real world worth.

1.1 The Gaming Industry

The gaming industry today is a multi-billion dollar industry that allready in 2004 [34] was reported as having overtaken Hollywoods film industry in revenue. Major title releases were outselling cinema blockbusters even then.

Out of all the segments of the gaming industry it is online gaming that is the fastest growing. While it is still a small portion of the gaming industry revenue as a whole, the increasing availability of low price broadband internet access is credited with the massive growth of the MMORPG segment. Since 2006 that segment has grown by 20%-25% each year [11] and Screen Digest's forecasts from 2009 shows this as continuing until at least 2011, having doubled its share of the total gaming market from 2006 to 2009. [40]

The gaming genre called Massive Multiplayer Online (MMO) or MMORPG (Role Playing Game) was named so by the creator of the first game to popularize and commercialize it, Ultima Online [64] in 1997. The genre sprung out of its roots in the early text based multiplayer game MUDs [65]. The 1996 Meridian 59 can be said to have been the first MMORPG 3d-game, but it's popularity and commercial success were marginal at best. The 1999 Everquest [60], in full 3d, is widely accepted as having opened the genre up to the public. Origin Systems reported their subscriptions peaked for Ultima Online at 250,000 and Everquest peaked at under 500,000. There are a few other important titles in the years that followed, but most important is World of Warcraft.

The market leading company in online gaming today is the California-based Blizzard Entertainment [57] with their 2004 hit World of Warcraft. As of a press release of late 2008 they had at that time surpassed eleven million active subscriptions to World of Warcraft [3]. Each of which are paying a monthly fee, this monthly fee and the way in which it is collected varies depending on the country of the subscriber ($15 in the US, €13 in Europe, much less in Asia), but a conservative estimate of an average of $7 per month puts Blizzards revenue from World of Warcraft, before including income from the sales of the boxed games and expansions themselves at over $900 million per year from this title alone.

When Blizzard merged with Activision in december 2007 their estimated value was announced to have been $8.1 billion and operating with a $1.1 billion revenue and a $520 million operating profit. [2] And allthough information is sparse, we at least know that their subscription-base has increased by several million since that time.

Allthough Blizzard Entertainment is in a unique situation in market share and revenue on their title World of Warcraft, the trend since year 2000 has been clear. More and more people are playing online games, and more and more online games are being produced. Even game types that were previously local or tradionally aimed at single player are introducing components of the game only available by connecting to an online server. Game developers such as IGN offer a competative or cooperative mode of gameplay while connected to a game server or additional content available through download.[31]

One reason that these games are all being developed with an online component is to try to battle internet piracy of intellectual property. The digital protection of products are getting better and better, but they are also becoming more complex and more expensive. And the games are still being pirated and downloaded. With an online unlocking required, or at least an online component or downloadable content avaialable to those who register, game designers are hoping to stear customers away from pirating their products.[33]

Since Xbox360 and Playstation3 even consoles have been entering the online realm, both competitors offer extensive services through their respective networks including downloadable content, score boards, online servers for multiplayer, game updates through patches and much more.

CEO of the merged company Activision Blizzard, Bobby Kotick, said under a speach at the Deutsche Bank Securities Technology Conference that ”‘...the 25 per cent operating margin business - has the potential as we can see with World of Warcraft to be a 50 per cent operating margin business. What used to be a low 20s return on invested capital business is now growing to a plus 40 per cent return on invested capital business.”’ He also explained how their business model would ensure increased returns on games like Guitar Hero: ”‘you might buy two or three expansions packs, different types of music. Over the life of your ownership you'll probably buy around 25 additional song packs in digital downloads. So, what used to be a $50 sale is a $500 sale today.”’ [7]

The net effect of this is that more and more games, and therefor more and more gamers are connecting to online servers continually. The threshold for registering accounts and using online services is being lowered. Allthough the *persistant* client-server-relationship is today mostly exclusive to the Massive Multiplayer Online games, the trend is showing that in the future this might be true for a much larger segment of the gaming industry. And where there is a persistent connection, the possibility for persistant states such as scores, affiliation and ingame resources become a possibility. And when these ingame possessions are tradeable and have a value to other players, they become a potential target for theft.

1.2 Virtual Economy

In a persistent online gaming situation your success and progress is measured and stored so that you yourself can review it or compare it with others. In an MMORPG the game is arguably about progressing your character in a persistent world. Your actions gain you experience and your experience accumulates into levels and strength or power. Also your actions earn you items and wealth, usually in the form of powerful items that further strengthen your character and in the form of items that have a measurable value in its ability to be used in producing some end result. Finally the games have their own currency, a set of money, commonly gold or credits or any other variation.

This wealth and power is both valuable relatively to the wealth and power of the other players, but also absolutely towards some measure set by the game designers. When it comes to wealth this means that you will need a set amount of it to pay for certain costs set forth by the game; training costs, purchase of readily available weaponry and so forth. But beyond this, the wealth is a relative measure between your wealth and that of other players. Just as in real life the money has a relative value compared to how much of it the other players have. If you wish to buy some item or service from another player, you will most likely have to pay for it by trading him some other item or amount of currency. The amount determined by supply and demand.

In fact in some games this meta-game involving trading and reselling commodities and crafted goods form an emergent system of economics subject to supply and demand, inflation and monopolies. For some players participating and turning a profit from the ingame trading becomes the main interest allmost to the exclusion of other aspects of the game.

This complex and emergent system of interaction between the players in games as far back as 1997 has been studied and shown to be comparable to real world economics, it is subject to economic theory in those cases it follows a set of requirements to the system. [16]

1.3 Real World Value

As players envy eachothers possessions and their own access to certain high value items is restricted, these virtual items have a value to the players. Players who stop playing sometimes sell their accounts, containing their characters and their items and wealth, to other players who value the accounts because of the time and effort put into them. Accounts are commonly auctioned off at sites such as ebay, allthough the major markets for reselling accounts are being pressured by some of the game companies to restrict the sales of accounts. The most paid for any character reported in the public was in September 2007 when a max-level, well-geared World of Warcraft character was sold for £5000, around £8500 at the time [17]. We do not know if this is the most anyone has payed for a character, and it's hard to calculate the total annual sizeof the account trading market, since most games come with a terms of use agreement that prevents the trading of accounts and hence such sales are done strictly off the books. Account sales can be difficult to notice and prevent, depending on the technology and software tools available to the game moderators, but only a few companies actually allow it.

Some ingame accomplishments take a long time, reaching the maximum level in World of Warcraft is currently estimated to take from 200 to 600 hours of game play. And for the majority of gamers these games really only begin once you are at max level. Other accomplishments require skill, great ability or extreme dedication, often seperating a few hundred players worldwide from the millions of others in the game. As there are gamers who want these ingame accomplishments, but don't have the time or skill necessary to achieve them, their percieved value of the ingame status can be linked to real world value, and players are paying real world money for them.

A large portion of gamers today are grown men that used to play as teenagers, but today have well-paying jobs and less free time. Their income lets them spend money on what their free time won't let them accomplish themselves and the industry of reselling virtual goods is still growing. Some of these games have aspects to them that people may find tedious and unrewarding, only the end result may be very rewarding. Exceptionally repetetive tasks, or especially completing the same time-consuming task on your second character, is often seen as necessary work to get to the level of play that is interesting and rewarding. Certain parts of the game may not feel like playing a game at all, but more like a tedious and boring job. As long as there is someone who is willing to perform that ingame task for you in return for a monetary compensation then there will allways exist a relation between the cost of having someone perform the task for you, the time it would take you to perform the task yourself, and the value of your own free time, or the potential earnings were you to spend that time at your actual job. These tasks, or the ingame items rewarded from them, are available to be delievered to you ingame by someone else if you order it via a third-party, paying with a credit-card on their homepage or similar.

The company IGE Ltd was started by two players of the 1999 Everquest. They sold ingame items and currency as well as providing ingame assistance to players who requested it, for money. Their company was based on profiting from players willing to spend money on improving their gaming experience. They were one of the first to start out in the market, and made alot of money selling virtual items to players. After expanding their market to several games, and setting up offices in Hong Kong with minimal-wage Chinese workers acquiring the items for them in MMO sweat shops, they started losing money in 2006 when the game developers increased their efforts to halt trades, delete accounts and ban participants of currency sales. The inventory of virtual goods lost from accounts deleted was costing the company alot of money. They were allready losing \$500,000 annually when a gamer from Florida sued IGE for ruining the enjoyment of the game for the million of players that were affected by the schewed economy attributed to the selling of virtual property. [26]

Allthough the original IGEs founders and original company didnt survive, it was bought by competitor Virtual Economies [37] and the market for reselling virtual property is larger today than it ever was. The amount of workers in China acquiring virtual property for these companies surpassed one hundred thousand [19] working out of sweat shops set up with shifts operating twenty four hours a day. And the people making the money from the sales are shielded from law-suits like the one against IGE by seperating the companies that acquire the items from the ones that sell them, and from basing shell companies in a series of other countries.[26]

Not all companies restrict the transfer of virtual property on the basis of real world sales, there are some that condone and even some that mediate such sales. Both the norwegian MMO developer Funcom, and Sony Online Entertainment were early partners in the startup of the company Live Gamer, a company that amongst other things provide an easy way for game developrs to charge money for ingame benefits and items via microtransactions. The extremely popular and wildly successful Facebook application FarmVille [61] is a good example of this type of application, it is free to register and use. Its revenue is generated by the players willingly purchasing additional farm equipment, livestock or bonuses. These items can be traded amongst friends or given as gifts and so have a measurable real world value.

In the virtual world Second Life, inhabitants can earn the ingame currency Linden Dollar in a variance of ways. The game seperates itself from many other MMORPGs in that the activities mostly mimic those one would expect to partake in in real life. Socializing, setting up shops, decorating houses and creating a community. But renting an apartment costs money, as does clothing and fashion items. Anything a player produces can be sold to others in the game, and you can make a profit if your products are popular. Especially those that buy land areas, residentialize them and rent out real estate to other players make a more than decent profit. [54] The creators of Second Life, Linden Lab operates a stock exhange of sorts called the LindeX where ingame Linden Dollars can be bought and sold for USD. In fact several players are making a profit by playing the game Second Life, cashing out in excess of one million USD in a year. The top earner was reported to have cashed out over 1.7 million USD in 2009. [53]

One of course has to pay tax on all earnings, even those made by selling ingame property. In addition, the question has been raised both in the United States and in the United Kingdom whether or not taxation should be possible on virtual property even before the profit has been converted to real world money. [35] [12] The link between the virtual properties and their real world value is becoming stronger as more and more people appreciate the relation. At least one can no longer deny the fact that virtual property really has real world value.

1.4 Virtual Theft

Just as theft occours in real life, it also does in online games. Deliveries promised don't show up or an agreed upon trade gets cut short before payment is fully made. Or someone simply picks up something that is not his, logs off and the item is gone. In some games these things are supposed to be a part of the game, and in some games they are moderated to the extent that a game representative will reimburse or handle a dispute between to players.

Instances of ingame theft have even provoked real world attacks; a Chinese player of the game Legends of Mir 3 stabbed a fellow player to death over what he claimed was the theft and subsequent sale of a magical dagger. [52]

These instances of ingame theft or scams are not rare, but they occur on a small scale, the invested time is rarely worth the potential gain and not easily repeated. Most occuring in the realm of single players looking for a quick boost to his own gaming experience. But there are player accounts in these games with virtual property on them worth thousands of dollars and if you can take control of that account, if only for a short period of time then you can take control of these items.

When you gain control of an account all you need to do is liquidize its assets before the owner or a game moderator can stop you, and you may be able to get away with the profit in real world cash. Accounts hacked in the game World of Warcraft are emptied of all their possessions in a very short amount of time. The items that are not tradeable are sold to a computer-controlled vendor for a lump sum of gold and the valuable tradeable items are traded, together with all gold, to another account. These items are then spread by trading to a number of different accounts and the valuable items are sold at bargain prices at an ingame auction house or by simply announcing the willingnes to sell the items in a crowded area in the game. If the prices advertised are low enough the thief can sell of all the stolen property in a very short period of time. This gold is then transferred to one or more accounts affiliated with a gold selling company who will try to sell the gold on hand to other players for real world money. A quick google search for "‘wow gold"’ quickly tells us the rates of buying gold at any server, the current price seems to be around €1.5 for 1000 gold.

Hacked accounts are becoming a serious issue in some of these games. The exact number of hacked World of Warcraft accounts is not published by Blizzard Entertainment, but it is easily verifiable that this is a major concern. A google search for the string "‘world of warcraft account hacked"’ yields an astonishing 191 million hits. Interviews with a group of players from the game revealed that among the fifty spoken to a full 22 had had their account hacked and emptied at some time since they started playing. Fifty out of the fifty agreed that this was a major concern and had been so ever since the game's first year on the market. Every single one of the people asked knew at least one other person outside the group who had had their account hacked.[1]

Blizzards own web pages for World of Warcraft advice their players on the relation between accounts being hacked and the selling of ingame gold stating that "'We regularly track the source of the gold these companies sell, and find that an alarmingly high amount comes from hacked accounts."'[15]

It is interesting to note here that while the game developers can see that the gold has exchanged hands and they can statistically see that the "'hacked gold"' is being reintroduced into the economy, it is really hard to satisfiably prevent this behaviour. It's all a question of resources and tools. Monitoring and seperating the normal game behaviour from the illicit behaviour takes time, money and server resources. Preventing the situation from arrising seems to be the preferred choice of countermeasure. Allthough efforts are being made across the board.

Hacking an account is a viable means of profit as long as there exists some way of taking the contents of that account and turning it into real world money. In the case of the gold sellers the money is transferred to a company by credit card and that buyer receives some amount of ingame currency traded to him by another character. Profit has been made.

2 Threats and Security

In this part a few basic ideas are defined that are necessary to frame the further discussion. Definitions on what sorts of threats and attacks that this paper focuses on, as well as a short indication of the scale and importance of the problem are stated as a starting point for the rest of the paper.

2.1 The Motives

In regards to taking control of someone else's account without their knowing or consent, hacking that account as it's called, there have been some studies on the motives of these attacks.[8] Looking at those finds in the context of this paper there exist four main motives.

- A) Accessing someones account in order to learn some piece of information that's stored there. This is extremly unlikely to be the motive for the hack of any gaming account except in the most unusal circumstances.

- B) Accessing someones account for the purpose of using the contents of that account within the game. This would include someone pretending to be the owner of the account for his social standing or inferred access to some activity or group. This is also unlikely, and as in the case above would be done in the situation where you have a particular target in mind and want access to that specific account.

- C) Accessing someones account with the intent of disrupting the game. The damage one can do after getting access to an account is substantial in any situation and if one can get access to a large amount of accounts it is possible to ruin the enjoyment of the game for a large group of people. This would be a stricty destructive motive and should not be a problem on a large scale unless some personal grievance against the game or game developer existed or it was done to undermine a competitor in order to win market share. The first is unlikely in its ability to finance any large scale operation and the second is also unlikely because there are many other and better ways of foul play in a competitive business. A simple denial of service attack would probably be alot more efficient. However the security of accounts against a purely malignant attack is still a major concern.

- D) Accessing someones account for financial gain. If the contents of the account, or the information stored there, has some value to a third party there could exist some way for the hacker to profit from being able to access other peoples accounts. In the case where the contents of any and all account have some value the hacker could attempt to gain access to as many accounts as he managed to and turn a higher profit the more accounts he was able to access.

There is a fifth important motive that must allways be recognised for hacking. Someone hacks another account simply because he can. It is an exercise of skill and is seen as a challenge to a certain group of people. There is usually a form of social standing connected to the action. While this motive is no less likely in the context of a computer game, the damage caused by a successful attack would be less disastrous simply because the motive does not include any form of disruptive action. However as this person is likely to want recognition for his achievement it is likely that he attempts to create an effect that will be reported and can be measured. In that regard the effects can be compared to the ones seen in motive C and if done in a large scale then the motives and observed effects may be seen as the same.

Both situations A and B concerns the hacking of a specific account in order to get access to some very specific property of that account.

Situations C and D give particular cause for concern for the game developer. Particularily because of the disruptive nature of both of them should they succeed. The fact that they would both be more successfull the more accounts they were able to hack means that any successfull attack would further increase the threat. The problem would grow exponentially based on its own size and success. For this reason these are the motives that this paper focuses on.

2.2 The Attacks

In the interest of this paper it is necessary to make the distinction between two different attacks or hacks, the social hack and the remote hack. This two types will be defined as:

The social hack will be the situation where the adversary knows the target. He has chosen one specific, or a group of, people. In this case the adversary might have the option to read through notes with passwords on them, use the same computer as the target, or steal his authentication code generator. It requires some form of physical proximity or trust with the target. This will not be concidered as major security concern in regrds to computer gaming in this paper. In the case where it does happen it would usually be personally motivated, usually A or B from the chapter on motives. It uses physical access to some piece of information or property from the target. Avoiding the theft or abuse of personal property is beyond the scale of this paper, it would most likely fall under the jurisdiction of local police.

The remote hack is alot more interesting. It assumes that no physical contact between the adversary and the target is possible. This would be the case where an adversary choses a target at random or from a list of people associated with a given service or web page. The adversary's information about the target is strictly limited to what can be gathered remotely. When concerned with the adversary operating under motives C or D this is the form of attack that should be emphasized. All the targets are anonymized and the objective is to break the security of as many of them as possible. With as little effort as possible of course. Any strategy to break the security of an account in this manner can be generalized to work on any account. This is the type of attack that this paper will focus on.

2.3 The Threat

While the threat to online gaming accounts may at first seem negligible, reports show that the problem is much more than a nuisance. Security company Symentec reports an extraordinary find from 2010/citesymantec:44mill, describing how they followed a trail of suspicious data that lead them to a database containing log-in credentials to more than 44 million online gaming accounts spread among 18 different games, predominantly asian games not distributed to the western market.

These were credentials that the owners of the database had gathered through an array of malware, phishing attacks and more and were storing for later use. Additionally they were operating a Botnet[58] to perform the actual validating of the credentials as well as the log-ins to perform some of the illicit actions once the compromised accounts were verified. This allowed the operators to verify and utilize the large number of credentials without being traced or blocked due to extraordinary traffic originating from only a few IP addresses.

While this discovery was quite extraordinary, it is not unheard of for some operators to be in possession of large number of log-in credentials. The contents of the gaming accounts are valuable and those in the business of realizing that value will pay for any verified account information.

The same security company, Symantec, releases security reports detailing the black market value of a variety of personal information types. Their report of March 2007 stated that while a fully compromised botnet-computer was worth between $6-$20, and verified credit card-information from the United Kingdom was worth between $2-$12, a verified World of Warcraft account was selling for $10. [49]

Clearly these black market prices can not be assumed to be precise values, but it can be assumed that whoever are buying these accounts are not paying more than they expect to make off them. It is, at the very least, a clear indication that there is a market for illicitly acquiried gaming accounts.

2.4 Security Minimums

The gaming industry is big business, and the developers of online games are large and serious corporations. Even the smaller developers are backed up by or have partnerships with large publishing companies. The de facto standard in the security of these games can be readily observed in all major titles and include, but are not necessarily limited to:

- Enforcing a strong and/or sufficiently long password.
- Limiting the number of failed login-attempts per time period to prevent brute-force methods.
- Choice of sufficiently strong cryptographical protocols and key-sizes.

These are the minimal security efforts that will be assumed for the remainder of this paper and all discussion that follows assumes the existence of these.

Additinally common practices include:

- Digital certificates or signatures proving the identities of the servers the client communicates with.
- A seperate and dedicated authentication server handling all account logins, authentications and authorizations before the connection is passed on to the dedicated game server or related web service.

All of these are well documented and thouroughly tested security standards from other industries. They are a proven benefit, but, as we will see, not necessarily enough on their own. This paper will assume that current best-practices are being applied in regards to these security schemes and analyse what further steps may be necessary.

3 Industries with Comparable Challenges

This part is dedicated to examining the main differences and similarities between the online gaming industry and other industries facing comparable challenges.

Particular effort is made to make clear the different legal situations that seperate the industries as well as the difference in user expectations user-proficiency between the gaming industry and other industires.

3.1 Examples of Other Industries

The online gaming industry is not alone in having to take account security seriously, their challenges are comparable to other industries, but their legal status is somewhat different and the priorities of the users differ slightly as well.

Electronic banking, especially web-browser based banking services, is very comparable to the online gaming industry. They also require a secure authentication that can be relied on to prevent unwarranted access. Banking web sites today commonly use at least one of four additional security measures: an authentication chip, a smart card, a one-time pad and a one-time code transmitted through a seperate channel (commonly an SMS to a mobile phone).

Official, governmental services such as the Norwegian Altinn[55] or similiar web sites handling sensitive matters like tax decleration, official applications, national registration and potentianlly electronic voting. Arguably these services require even more stringent security measures and very commonly utilize a smart card and a one-time pad. An authentication chip is being used in few countries.

These are all examples of log-in requiring something seperate and extra on top of a simple username and password. There are countless different ways of delivering or implementing this extra bit of log-in requirement and they shall be further discussed in the later chapter on Two-Factor Authentication.

Ultimately any industry or service that offers the user a way to remotely, and through interaction with an automated system, to perform some sort of action will need to consider the same challenges and options as the online gaming industry faces in regards to security and user authentication.

While the requirements seem comparable in these cases there are still a few key differences. First of all the security requirement of a game company relies solely on its own perceived gain from an increased security. Primarily only once a threat to their product has the potential to lower or destroy revenue is an increased security is appealing. There is a fine balance between cost and gain.

The security requirements of banking and governmental services are governed by laws and regulations of the countries in which they operate. The information they carry is potentially sensitive and security is paramount, useability and cost are secondary considerations. Contrary to the gaming industry there exists a zero-acceptance of breaches in security.

3.2 Legislative Differences

Legislation is mature and well-established in the cases of acquiring another persons bank details and withdrawing his money. Digital crime has existed long enough that most states take the invesitagion and prosecution of bank fraud and the like serious. Any attempt, failed or successful, to hack a web-based banking institution would surely result in an investigation if it were detected. Virtual crime as it pertains to gaming is an entirely different matter. Its very definitions are in their infancy. The very ownership and real world value of virtual items are disputed. Most online games except Second Life actually state in their End User Agreements that any and all ingame poessessions and associated benefits of the accounts operated within the game are solely the property of the game company. All you own when you buy and pay for your account is the right to operate and use that account.

Still this does not change the fact that real world money routinely changes hands when ingame property is traded every day. When US. Joint Economic Committee stated as early as in 2006 that they were looking into wether or not virtual property would be taxable it was an indication that this area of legislation would likely be open for revision in the years to come.[18]

South Korea is one of the countries in the world with most active gaming population. Gaming tournaments are played live in large stadiums and their participants are treated as star athletes. Their police handle virtual disputes and thousands of virtual crimes are reported every year, as many as 22.000 in the first six months of 2003. [32] But South Korea is an isolated example and most other countries have not historically investigated reports on crimes of a purely virtual nature.

This is changing, however slowly. In 2008 the new British Police Central e-Crime Unit was set up and in November 2009 a man was arrested for "‘hacking into accounts to steal virtual characters and their possessions"’. [36] And in the Netherlands two minor boys were senteced to community service after physically forcing a fellow class-mate to digitally hand over his ingame possessions. The court ruled that "‘these items are valuable to their owner and he has been forced to hand them over to somebody else, it should be considered theft"’.[24]

However, fact of the matter is that those that engage in stealing gaming accounts still operate virtially without fear of prosecution. Techniques like operating from within certain countries, hiding ip-trails, using a distributed system or in the extreme cases operating a botnet [58] are just as available to the perpetrators of virtual-game-crime as those targeting banking institutions. And without extensive cooperation across borders or using massive resources, the investigation of these matters are very difficult. Even if it were to be attempted.

No security measure can be 100% safe and without the fear of prosecution these operations are becoming extremely aggressive. Trojan worms and phishing attempts is a daily threat to many of these gamers. The operations are large scale and very intrusive. This is the main difference between the security threat of the online gaming industry and other comparable industries. The threats are open, aggressive and relentless. They don't pop up once in a while as is the our experience with attacks on banking services. They are an ever-existant and constant threat.

3.3 Different Use Patterns

There is no point in having a secure system that nobody ever uses. In order to have a successful and secure system you need a security system that fulfills your security needs and that the users will accept. Because of this the security profile of a system needs to take its users into account. While the demographic of gamers is diversifying, there are still valid generalisations to be made about the people that play video games. A significant portion of gamers are males in the ages 16 to 34 with several recurring themes in regards to education and shared interests.[22] This is changing, in some cases, such as the increasing number of women playing in more and more female-friendly environments, rapidly. [13] Any game will nevertheless have a certain social selection of users that it is catering to. This is in contrast to some of the comparable industries where you might have users of vast variety, or everyone, among the adult population of a country or region. Ultimately, a game developer *choses* its target audience as it develops its game, a banking institution does not have this luxury. This fact can be used to tailor a security scheme to that particular target audience.

This difference from financial or governmental institutions gives some advantages to what you can assume your users to know or be comfortable with. Some developers might rightfully assume a certain level of technical competence amongst it users and utilize that to implement security features that would have been cumbersome or unfeasible in other systems.

There are challenges as well. Notably the habits of the gamers and their expectations of when and how they should be able to access the game. A bank application or a web site for tax decleration might be accessed by a single user from as much as once a day to about once a year whilst some players in an online game will access their accounts up to several times a day. Many of them every day, and at all hours of the day. This potentially reduces the usefulness of any security scheme with a significant cost or complication per log-in. Depending on the game or audience there might be extreme demands on portability and client-transperancy.

As players of World of Warcraft have shown with the introduction of their Authenticator Chip the players are sometimes willing to accept more than the developers first expect in order to secure their own accounts [51], but some security schemes might prove to stringent for the users. As video games in South Korea are mostly played from internet cafes, having a security scheme that prevents you from accessing your account from more than one computer would be an unimplementable feature, but the same scheme might be a good choice in the case of a game designed for a mobile phone where the user is allways accessing the service through his own phone.

Additional security in a product has no benefit if it also increases the complexity to a degree where its users lose interest, or the cost to a point where it's not able to sustain itself. Ultimately the choice of security schemes should be made depending on what the intended users of the product are expected to accept and handle. This is particularily true in the case of video games.

4 Security Schemes

Following is a description of several methods of additional security in use by the online gaming industry as well as other industries facing similar challenges. Included in the presentation of each scheme is a discussion of their strengths and weaknesses, both those specific to the online gaming industry and those cases where the it proposes an exception to the experiences of the other industries.

At the end is a description of Two-Factor Authentication and its value and importance.

4.1 Recovery rather then prevention

As has been stated time and time again, no security scheme is 100% safe. It is a well-accepted truth in the industry. All you can do is minimize risk and potential harm. Since for the vast majority of the users, computer gaming is a recreational activity, the potential harm is often viewed as very limited. As such many companies have chosen a cheap, and easy to use, weak authentication scheme and instead focused on correcting and reverting the unwanted changes done in the game by those that manage to achieve access.

The major game developers have a dedicated customer service department dealing with compromised accounts, making sure they help as many customers regain control of their account as possible in order to not lose those customers. Sony Entertainment, Mythic Entertainment, Funcom and Blizzard Entertainment and more are all very open in their policy on what is necessary to recover a compromised account and in their communication with their community on the problems and the recommended precautions. [10, 9]

The recovery of a compromised account has become routine for these companies as accounts are hacked every day, and the problem is not showing any signs of fading.

The companies will do whatever is necessary to restore the account to its previous state in order to please a disappointed customer. Backup-databases, event logs and player descriptions are used by the game administrators to restore the accounts so that their customers will not suffer unnecessary. In order to prevent false claims of losses of powerful items the customer may not have owned at all the game administrators rely heavily on server logs of transactions and events to check the stories of the user. Using these server resources the recovery teams can restore allmost all accounts that have been compromised and return the account to the original owner by validating their identity through additional security implementations such as faxing identification or passports, or anwering secrity questions established at the account's time of creation.

In the overwhelming majority of cases this means that the customer only suffers a small window of unavailability and no permanent damage. But the recovery process costs money for the administrators. Verifying user reports to catch false claims and getting all details right when restoring the account requires a staff dedicated to the job as well as an expensive set of tools to be able to manage and search the logs and databases.

The complexities of these MMOs can be enormous, a single character can have large inventories, banks, relationships, specialisations and a detailed statistic of performed actions or abilities. Each character consists of a significant amount of data, the databases of these games are very large indeed. If a character is wronfully deleted there needs to be a backup so that it can be retrieved from a previous state, and all backups add to the complexity of the system.

But the system needs backups anyway to deal with potential system crashes or any other events, so being able to restore a character or account to a pre-hacked state is deemed an acceptable increase in system complexity. However, tracking the stolen goods is not so easy as it would at first appear.

The root of the problem with hacked accounts is that the hacker is able to get away with possessions and in-game wealth. This wealth is redistributed to other characters and ultimately sold off to other users. All of this happens on the game servers, and all transactions are logged. It seems strange then that they are not able to adequately seize all illegally attained assets. The complexity of tracking the transactions in the logs increases so quickly in fact that it's proven not worth the time. By spreading the wealth out over a number of accounts and using a large number of transactions, actually following the trail of the assets becomes too hard to do satisfcatorily or quickly enough. They do track the assets to a degree and they do take action on a regular basis, it's just not enough. They need to be very careful not to ban anyone innocent, and it might not be in the game company's best interest to warn or ban a player that just got a large amount of gold transferred to his character. Even if that player is in breach of the terms of use by purchasing gold from third-party companies he is still a customer that the game company is making money off of.

Restoring a character to an old state is easy, but unwinding the complex chain of events that characters possessions has sat in motion after leaving its account is unfeasible, so in reality the game server ends up with double the amount of wealth available because it restores one character with his full wealth without removing his previous possessions from the game world. This works in a small scale, but if the problem becomes too great the impact on the in-game economy becomes noticeable and problematic at the same time as it doesn't erally prevent the attackers from achieving their goal.

Experiences by members of the group I interviewed from World of Warcraft indicated that the response-time for dealing with compromised accounts, incidents where the account had been hacked and completely emptied of all assets, was improving on the average. Those who experienced getting hacked in 2005 reported several emails and lengthy communication via email or telephone with Blizzard representatives and two to three weeks waiting period before their accounts were fully restored. This is in drastic contrast to the more recent experiences where response times this year were as low as three hours after initially reporting it via an in-game help menu. [1]

The problem of comprimised accounts in World of Warcraft noticeably flared up in september 2006 when a couple of new Trojan and Malware programs surfaced targetting their users. The customer service department got so bogged down by the increased demands that their telephone lines were closed for an extended period of time.[28] When the problem grows to this magnitude the choice of recovery rather than prevention becomes less than desirable because of the increased cost and unsatisfying user experience.

4.2 Simple Password Scheme

At the very basic level of security the account will be closed to everyone except the poerson that knows the password combined with the username. This password is not necessarily simple, valid practices include a minimum of eight characters of at least two of the groups small characters, large characters and numbers, and is not recognized as a dictionary word. The term simple is only to signify that the security scheme requires no other information than the username and the password. Should a third party acquire this username and password he would be able to have full control of the account.

It's a long time since this security scheme was deemed lacking, and it is rarely ever used in vital applications or services anymore. It is however still a dominant choice in most games or gaming accounts. The security of this scheme is inherently flawed as the password can easily be read from over a shoulder at the workspace or because users tend to write them down on post-its or in text files on their computer. Phishing [62] is the ultimate nail in the coffin to the simple password. The technique was first described in 1987, and the first recorded phishing attacks are from the mid 90's. [25, 48]

Collecting an accounts username and password information is by and large very easy. The average user will just as easily give his password away to an unknown person claiming to be a system administrator for the system in question. Or he will be fooled by an equally-looking web site with a slightly different URL that is actually an adversary masquerading in order to snatch passwords from unsuspecting users.

Many users use the same username and password combinations on a vast number of different services. Often also on services with extremely lax security measures. One comprimised web site can provide the hacker with a full database of username and passwords that they try on other services and web sites. One recent example is the compromise of the protocols of music streaming service Spotify that might potentially have led to exposed passwords. Spotify advised its users to change passwords on all services that shared the one that had been used with their service. [41]

Finally the presence of a key logger on the computer renders this security scheme absolutely obsolete. Key loggers come in a variety of shapes and forms, but most importantly they have existed for quite some time, they still continue to exist and they are constantly evolving and adapting. Through features such as Drive-By Downloads [47], it is possible to get a computer infected without necessarily clicking or installing anything - simly visiting the wrong web site can be enough.[46]

By now all but the most trivial systems have implemented additional security measures to counter the ease of which a password can be retrieved by malicious third parties, but the gaming industry is still mostly relying on their old password-protected systems. Their information is rarely sensitive and any consequences of a breach of security can be handled by themselves so they have not taking this issue seriously enough yet. However this is an increasing threat and especially because of the homogenous nature of the users of any given online game the infections from fansites are even easier and more succesful than against other comparable industries

What leaves the customers of an online game especially vulnerable to phishing or key-logger attack is the fact they they all share a very similar interest, the very game they are playing. Fan sites, news reports, tips and guides, gold selling web sites, video resources and sites with player interviews are all prime targets for someone looking to snap up a large number of account credentials. Simply compromise one of these popular web sites and you can infect a large amount of computers in the exact target group you want. While users of a web based banking service might share few or no simliar web surfing habits you can easily find common surfing habits among the players of a game as intricate and user-driven as for instance World of Warcraft.

This makes relying on a simple password driven security scheme for online games a very bad idea.

4.3 Server Certificates

Certificates are well known and effective security measure. It allows the signing of communication from a server so that the user may verify that they actually communicating with whom they think they are communicating. Given a reliable Public Key Infrastructure and Certificate Authority [63, 59] that is. This is mostly used to prevent phishing attacks in which malicious web sites masquerade as legitimate banking or financial sites. You're web browswer will give you a warning should you try to visit this false site because it's certificate does not match the one it expects to receive from that site.

These certificates, however, add quite a bit of overhead on the administration of the web sites and the useability of them. You need to download a new certificate on every computer and every browser you wish to use.

A malicious site might sign its own certificate and the user would only realize the difference if they actually checked the certificate information. The fact that most users suffer from what is known as Click-Through Syndrome and they generally don't wish to be hassled with checking these things certificates are less effective than desired.

For these reasons the Norwegian branch of the Swedish bank Skandiabanken AB no longer uses the certificate scheme that they had been using since their inception in 2010, citing unnecessary overhead for users and administrators and the end users.[44]

There is no uniform adaption of a known certificate scheme in all major online games, however they do mostly use public cryptography practices to sign and negotiate connection initiation and session keys for encrypting password transfers etc.

In the case of computer games the clients you log in with as well as the servers you log in to are owned or run by the company that developed or maintains the game. The connection information is stored in the client and there is little reason to doubt the validity of the receiving server, even without a certificate. If the client has been compromised then this problem is moot as there are bigger issues to deal with, as shall be investigated in a following chapter.

One possible idea would be to require a *user* certificate on the client computer that included a key necessary to connect to the game server. No one could connect to your accout without knowing your password and being in possession of your user certificate. This is not a bad idea and should be considered for some specific services.

The main problem with this security scheme is the necessity to re-download the certificate should you accidentally delete it, reinstall your computer's operating system, buy a new computer or wish to play at some other computer than your own. What should be the necessary credentials to download your certificate. It needs to more than just your password and username or else whoever used a key-logger to glean that information can now easily download the certificate himself and proceed with this attack. One could require faxing of passports, or telephone-verification of security questions, ora waiting period or any of a number of security schemes to validate a users right to re-download a certificate, but any satisfactorily safe method adds a complicating overhead to the process that makes it impractical for the user to quickly install and play the game from any other computer than his own. This might be acceptable to some users or to some games, but for many others it would be an absolutely unfeasible security scheme.

4.4 Two-Factor Authentication

Two-Factor Authentication is a specific case of an N-Factor Authentication wherein you require a user to authenticate using two of the following things ”‘Something you know”’, ”‘Something you have”’ and ”‘Something you are”’. The reason for wanted to add a second factor of authentication is that if ever one of the factors is compromised then the security of the account should still be sound as long as the other factor remains uncompromised.

- Something you are can be examplified as your DNA, your iris scan, fingerprints or any other biometrically measured information from your own self.
- Something you know is the knowledge you possess, your password, username and any sercurity questions or other information that you might be able to pass along to someone else should you need to or be tricked to.
- Somthing you have is an item in your possession as in a credit card or your house keys. When increasing from a single-factor to a two-factor authentication this is usually what is added on top of something you know. There are many different options as to what it is the user needs to be in possession of in order to authenticate and some of them will be discussed later.

A necessary increase in security to deal with widespread phishing-attacks led to the norm in most banking institutions turning to what has become known as Two-Factor Authentication. The idea is not new, but its time of inception is not widely agreed upon. However from early 2000 several banks in Norway were allready using them. In 2004 US Homeland Security issued a directive outlinig its implementation of a Two-Factor Authentication and its importance for their new governmental id credentials.[39] An article on the subject from 2006 however shows that while many banks were implementing some form of TF-A, it was not universally accepted worldwide yet[5], while Microsoft announced at CeBIT in 2005 that they were going to fully abondon a simple password authentication for a two-factor authentication[50].

The User Certificates mentioned in the previous example can be classified as something you have. It is at the very least a seperate thing from what you know and hence classifies as a second factor. The main weakness to using this as a second factor is that the certificate is stored on your computer together with the very client you will be using to connect and enter your password. Keeping all your eggs in one basket like this is not a good practice and it will be very vulnerable should your computer be compromised.

A One Time Pad is an encryption-type invented at the beginning of the 20th century. It consists of a pad or list of keys that each are only used once to encrypt or decrypt a message. Without acquiring the list of keys it is impossible to guess the next key in the sequence. However Encryption in large scale with the OTP is very costly because you need a secure and seperate way to distribute the list of one time keys. It is however used today as a method of authentication in many banks around the world. It works by having the bank send you a piece of paper or card with a list of short codes on it and requesting one of these codes every time you wish to log in. There exists no way for anyone else to know the codes before they are used without physically gaining access to the code card, so as long as the card is in the users possession this method of authentication is considered secure.

However since it requires the distribution of the list of codes to the users in a secure channel seperate from the main channel used by the log-in itself it adds a significant logistical problem and cost per log-in that makes it costly for a game developer. Especially if operating in a large number of spread out countries delivering the code cards by mail, which is usually the preferred method, becomes prohibitively difficult

An Authenticator Chip is an authentication code generating piece of seperate hardware. It uses a seed key implemented at production time to generate a one-time code based on an internal clock. This code is only valid within some chosen period of time from when it is generated. Generally within a minute or so, to allow for user faults or input lag. And the code is cryptographically secure to anyone not in the possession of the generator key. As such the numbers generated can be treated as completely random rumbers as long as the implemented cryptographical protocols are sound.

This is becoming a very popular method of authentication. There is a small cost of producing the chips and distributing them, but once distributed they use very little battery power and a have a very long life expectancy. Norwegian banks charge about US$10 to replace one if you lose it and Blizzard Entertainments Blizzard Authenticator [21] costs US$6.50. However needing to keep the authenticator with you at all times you wish to be able to log in to the game is not well received by everyone. While many people opted to acquiring the Blizzard Authenticator for additional account security when it was released there were still the vast majority that did not chose to do so. Amongst the players in the interviews [1] only 19 out of the 50 were using the authenticator two and a half years after its release and a full 40 out of the 50 said that they would rather be without the additional chip. Citing reasons such as being unable to quickly log in to check up on or handle specific issues while visiting someone else that had the client installed unless they carried the authenticator with them at all times.

SMS-delivered One Time Code has been used for as long as the Authentication Chip. It works by sending a piece of short text-string to the users registered phone number using Short Messaging Service. The mobile phone is considered a seperate channel, and while it is not necessarily secure it is unlikely that anyone able to gather your password will also be able to intercept and decrypt the message sent to your phone. It is a widely used security schemes amongst banks, not far behind the authenticator chip, and since it relies solely on the mobile phone and no other possessions it is sometimes a preferred scheme. For some users keeping their mobile phone accessible is as second nature as remembering to eat. For a large amount of these users it is perfectly assumable that they will allways have their mobile phone when they need to log in and no larger risk of them losing it than losing an authentication chip.

There is however an increased cost associated with it. While you avoid initial cost of acquiring or producing the authenticator chip there is a per log-in cost for each SMS sent. This can be as low as 1 cent per message with the approprate deals with phone operators, but to establish deals with operators across a large number of countries or perhaps the whole world may prove prohibitively difficult. For an online game aiming at a global market securing these deals would add alot of extra cost and complexity. In some cases even politically difficult. Sending SMS text messages all over the world without a proper discount or delivery agreement would prove financially unviable, even within Europe sending simple text messages are several hundred percent more expensive to neighbouring countries. There are other security schemes that are much more suitable for a global market, but for a geographically limited service the SMS-code should be considered, depending on the amount of times the average user is expected to log in every day.

Secondary delivery system on same machine has been attempted in some rare cases. It is generally the same idea as resending your password to your email account if you have forgotten it. The idea is that before logging in you request a one-time password and it is sent to you through your email or some other instant messaging service or application installed on your computer. Hopefully to something that you can read or open on any computer without installing extra software, though this varies. The strengths of this scheme is that it does not require any extra hardware and it works anywhere. The problem is that if an adversary can get a hold of your username and password it is not so inconceivable that he also has access to your mail account or instant messager or whichever account the game will send its one-time code to. If the adversary has a key-logger or compromised the computer in some other way then this security scheme does nothing but add extra complexity. Once the adversary knows your username, password and credentials for logging in to whatever service will be transmitting the one-time code, he will be able to repeat the log-in process at any time from any location of his own choice. It does not sufficiently fullfill the requirements of a Two-Factor Authentication if the system is compromised and therefore does not fullfill them at all.

4.5 Authentication-code-generating Application

An Authentication-code-generating Application is a software implementation of the authenticator chip. It is an application that performs the same task as the dedicated chip without requiring the seperate hardware. The application could be installed on a smart phone or a laptop or any other platform that the user might be inclined to bring with him whenever he needs access to the service. You download or install the application to your platform of choice and use that piece of hardware as you authenticator chip from then on. Being installed on a general platform leaves the application much more vulnerable to tampering than a dedicated hardware authenticator chip, and any viruses or weaknesses that might exist on that platform will expose this application as well. This is something to be aware of, but it is not necessarily the bane of the scheme. The one-way cryptographic functions used to generate the authenticator codes would potentially be exposed, but their security is not reliant on the obfuscation of the protocol, only on the secrecy of the generator seed, the secret authenticator key.

This solution is bound by the same cryptographic principles as other cryptographic schemes. Even by observing a large number of generated codes it would be computationally impossible to calculate the generator seed and hence impossible to know any future authentication code. Even knowing a set of generator seeds and observing a set of randomly selected authenticator codes it would not be feasible to decide which seeds generated which codes without exhaustively testing the generator seeds. If your authenticator application is located on your main computer, the one you will be using to access the service, and this computer is compromised, then the assailant would have access to your username, password and could generate his own authentication codes. Consider however if the authenticator application is never allowed to be installed on a platform that also allows log-in of the service it is generating its codes for. Compromising the, for instance, smart phone, would allow the assailant to generate authentication codes, but he would have no way to know wich user accounts to use it with. The smart phone holds an ID and a generator seed, but the only link between that ID and the user account is located on the authentication servers, safely tucked away from prying eyes. The user knows which authenticator application to use to generate a matching authenticator code, but there should never exist any information on the computer or the smart phone or the information transferred to the authentication server that would allow anyone to deduce that link. Analysis of geo-positioning using the smart phone's GPS or network location together with the computers IP-address might provide some indication, but at the very least that analysis is extremely time- and resource-consuming.

In 2009 Blizzard Entertainment released just such an application for Apple iPhone and iTouch users. Available as a free download as an alternative to their previously released Blizzard Authenticator hardware chip [43]. In february 2010 they released an Android version [42] and they now support a large number of phones. In contrast to the hardware version their mobile authenticator is available free of charge.

Avoiding the production cost of an authenticator chip is one reason to consider the authenticator application, the other is its useability. By making a few generalizations about its customer base, and hopefully providing some alternative to the rest of its customers, a company can assume its users will have a readily accessible smart phone to act as an authenticator. One of the main issues with the hardware authenticator chip is the need to have it readily available at any and all times you might need to log in, if you assume the mobile phone is allways readily available then this concern is greatly alleviated.

While there is no production cost, there is is, however, a development cost associated with an authenticator application. It will need to be available to a vast array of different mobile phones or operating systems and provide potential updates, service and maintenance for them. There is, though, no reason why a single company needs to assume the full cost of this alone. There needs not be any proprietary protocols or algorithms, no service-specific differences. There is no reason why a set a distribution companies could not collaborate to provide a collective authenticator application. The user would only need a service-ID connected to the game and an account-specific generator seed for each product the application were to be used with. While Blizzard Entertainment is a large company capable or absorbing the cost of developing such an application on its own, this authentication application is a good idea for many smaller game developers as well. Especially because of its low production cost and its good scaleability once you have support for the important smart phones or required platforms.

One noteworthy problem with Blizzards Mobile Authenticator is that they presently are also releasing a plethora of mobile applications for other game-related services that require log-in. Their armory application and their auction house application are two examples where you log-in using your account in order to control aspects of that accounts assets. They even recently added the option to "'copy to clipboard"' the generated authenticator code so as to make it easier to paste in with your account information when logging in. This directly violates the idea of keeping the authenticator code generating application physically and informationally seperate from the process of logging in. As long as both the generator seed or code generating process exists together with the username and password, the worth of the second factor of a two-factor authentication scheme is reduced significantly. All it takes is a virus or a trojan to infect the smart phone and an assailant would have all the information he needs tocompromise an account. This is in my opinion the most important aspect and most crucial security hole to consider when chosing to use an authenticator code generating application.

There are however a large amount of different schemes for delivering a one-time code that can be used. Discussing them all would not be constructive, and there are surely more to be invented in the future that should be considered when become available. What is important is the extra security the Two-Factor Authentication adds and the impacts that it has on the security systems. The choice of delivery system should depend on the game and its intended audience. The fact that most of the target audience might have a mobile phone with them at all times is one fact that can be taken advantage of, but there are other things to consider and having several options to chose from should be seen as an advantage as a developer.

5 Shortcomings of Two-Factor Authentication

This part of the paper focuses on the exploration of the continued security problems even after adopting state-of-the-art security schemes like two-factor authentication. The very core of the problem that this paper tries to explore is explained as well as why such an imbedded problem in any industry facing security challenges.

The very things that have allready been explained as different from comparable industries are explored as both further weaknesses to the industry as well as potential strengths.

The end of this part concludes with a description of what should be an amply strong security scheme while still having the potential for failure against a sufficiently motivated adversary with abundant means and resources.

5.1 Authenticator Codes Subverted

There is a problem with the use of Authenticator Codes as the second factor of a two-factor authentication scheme. In principle you use "'what you have"', the generator of the authenticator code, to generate a token, the code, and you show this token to whoever you wish to authenticate with. Knowing that no one other than the owner of the authenticator code generator can generate that code, the target of the authentication will accept that you are in posssion of the generator. This is however not necessarily true.

We prove possession of the generator by calculating a token that only the possessor of the generator could calculate, this is in contrast to for example the physical possession of a key needed to open a safety deposit box in a banking situation. In fact you not need to have possession of the generator to be able to produce a generated code when necessary. The generated codes have a short time-frame in which they are acceptable. The time-frame is of course decided by the implementators, but in order to be user-friendly a value of 30-60 seconds is pretty common. This means that an assailant needs only be able to get his hands on a code and use it within this time-frame together with the username and password of the account in question to be able to falsely authenticate with the server.

One incident of the succesful subvertion of a two-factor authentication is from July 2006 when a phishing site that looked just like the web site to a company called Citibank in the US was launched. Users were prompted to log in by an email that linked to the page and the operators of the phishing site then used the credentials, including the authenticator code, to falsely authenticate themselves to the the proper bank site and transfer large amounts of funds out of the country to nations that don't extradite to USA.[27]

The weakness of the two-factor authentication was explained in 2005 by Bruce Schneier[45], and basically the security schemes fails as soon as either the user trusts some malignant site that is masquerading as the real thing, or the user has some trojan or other malware on his computer designed to piggyback or intercept and alter the communication between the user and the web site. The phishing-site example is a man in the middle attack with the adversary sitting behind the fake web site, and in the malware example the adversary is actually a program, or script, within the users web browser that sees and knows all the user is doing, and is altering the communication with the web site to serve his own interests. The assailant does no need to be in possession of your authenticator code generator, because he can sit undetected within the very tool that you use to communicate with, and he can alter any and all communication because he can also alter the responses shown to the user. A research paper from 2004 shows how a the securty scheme of German banks using one-time codes called TANs can be circumvented. [23]

The one big difference that seperates the security schemes utilizing a one-time code like an authenticator is the fact that an adversary cannot collect large amounts of user data and use that information at a later date to access all the accounts. The one-time codes he intercepts have to be used within a very short time window. This time-sensitivity of the information raises the complexity of the attack and the cost of an operation aimed at breaking the scheme, but ultimately does not add any actual securty benifit if the targets computer has been compromised. Finally the example of a malware from 2008 called the trojan.silentbanker [30] shows us that these adversaries do in fact have the time, resources and skill to exploit this weakness. The malware contained detailed instructions and seperate algorithms for dealing with over 400 different banking sites, not only in the USA, but also most European countries. [29]

5.2 Two-Factor attack in WoW

While attacks on second-factor authenticated systems have been seen in other systems, and they have been theorized and anticipated in online games it was not until february 2010 that the first attack was actually confirmed. There were rumours about accoutns with authenticators being hacked before this, but never of any large scale and not with substantial proof to indicate it was anything other than user error or a social hack.

However, the emcor.dll malware changed this. First reported in a post on the World of Warcraft Technical Support Forums [66] the dll file lets the adversary do exactly what we have seen in other similar attacks in other industries. Being spread through a large amounts of fake WoW-related sites installing it through drive-by downloads it unknowingly infected a large amount of Blizzard customers. In fact a large amount of domain names very simliar to popular WoW-sites were featured in google-ads when searching for that service on google, something many users are using instead of remembering exact URLs.[14] The simliarly named sites automatically installed a piece of malware, by exploiting a number of security holes in the user's browser, that subsecquently installed a file called emcor.dll on the computer.

The dll-file hooked into the system and intercepted username, password and authentication codes from the WoW-client, transmitting them to the adversary and subsequently crashing the game with a crash report to make the user believe his game software had somehow been corrupted and needed to be repaired or restored. Important to note is that needing to restore or repair the World of Warcraft software is not that uncommon and many users will do so without considering that there is a malicious piece of code making him hink he needs to do so. The dll-file thus stopped the authentication code from being transmitted and so the adversary was free to use it even though such codes can ever only be used once. [4]

The adversaries promptly used the information to log in, before the code expired, and transferred all resellable assets on the account to their own accounts before logging out and moving on to another account.

Blizzard Entertainment are correct in stating that their Authenticator was not broken, and your account is definitely more secure while using it than without it. It does provide safety from the pure keylogger-attacks. But they were mistaken in thinking that an adversary would not have the means or motivation to facilitate this sort of real-time second factor attack. Clearly the monetary gain from hacking online gaming accounts is sufficient motivation to initiate this sort of wide-spread and resource-demanding attack that requires real-time presence from the adversary.

5.3 Authenticate the Transactions

The requirement of one-time codes means that an adversary cannot simply log in and perform whatever actions he wants at whatever time he desires just because he knows your username and password, but should he be able to acquire one of the one-time codes he can log in at that particular time and perform said actions. Once logged in he has complete access.

The addition of Transaction Authentication is aimed at preventing this. The theory is that the user will try to log in, but the code is intercepted and the adversary logs in instead. Now the adversary will not be able to acquire further codes to re-authenticate when performing transactions because the user in possession of the one-time codes is not himself trying to perform any transactions.

The Silentbanker Trojan discussed in the previous chapter was a malware installed on the users computer that could subvert even this security measure. Even a phishing site can do this, though it is harder to accomplish in practice it is perfectly possible. The adversary performs a Man in the Middle attack where he allows to user to log in, with him cotrolling all the information from an intermediate position, and when the user wants to perform a transaction the malware changes the details of the transaction to transfer funds to some other account controlled by the adversary. The bank then asks the user to re-authenticate and confirm that he wishes to perform the transaction.

As long as the malware is in control on the users computer he can show the user what the user expects to see while telling the server what the server expects to hear. The user sees a request to insert an authentication code to confirm what he just typed in and he sees nothing out of the ordinary about the information he is confirming. The malware then uses that code to confirm the modified transaction.

In fact this is exactly what the Silentbanker did, but only if it had to. If the target bank only needed a password and username, it transmitted those details to its servers for later use. If the bank required a one-time code to log in then it used that code to log-in and perform whatever actions it wanted to. If, however, the bank required transaction authentication, and only if it did, the silentbanker piggybacked onto the session of the user and performed modified transactions. The trojan performed whatever actions the security scheme of the different banks allowed it to get away with.[6]

As long as the computer has been compromised you really can not trust anything it tells you or asks you to do. It does not help that the channel of communication between the computer and the server is secure if the computer itself has been compromised.

Interfaces of banking sites are easy to use, and generally very easy to replicate. The phishing sites take advantage of this by masquerading as the site you expect to see and the adversary trying to get you to confirm transaction you don't want to perform do the same. The user does not react to the presence of the malware because the malware is able to replicate the behaviour of the web sites so well.

5.4 Authenticating Transactions in a Game

Replicating the behaviour of an online game is a lot harder. In fact, altering a game client without it being detected is pretty hard. Launcher applications have become the adopted standard the last few years. They handle things like checking for updates, applying game pathces, providing news or information to players, and validating the game client before allowing it to run. Checksums are one of the means used to make sure the game client is valid and has not been tampered with. Fooling this check is a non-trivial task. The emcor.dll intercepted the communication from the network-protocol and used keylogging technology to acquire and reroute the communication to its modified target, and was able to crash the client. It was not able to actually change anything in the game files or provide the user with a modified game screen.

Consider if the game client allowed you to log into the gaming world, but asked you to provide an authentication code after you had entered the game. Your gaming would be halted in a momentarily paused state until you could provide the requested code. Only after having re-authenticated the user would he be released and be allowed to resume his gaming activity. He could also be allowed to perform some trivial non-problematic actions determined by the developers while waiting for the re-authentication. This re-authentication could be requested any time the user wanted to perform a set of critical actions or at time intervals, or simply a one-time thing after initial log-in.

The reason authenticaion of the transactions does not work adequately on a web site is that the user can be provided with anticipated information that he won't question, but if you logged into a fake gaming server provided by the adversary then it would be prohibitively difficult for him to convince you to re-authenticate because he should notice that things were not as expected. The lacking presence of guild-members in the chat channel or that the cities were presumably void of life would tip the user off to the fact that there was *something* amiss. This is of course assuming that the adversary was able to provide a game server that the client and user could connect to.

If the adversary is simply listening to what the user is trying to communicate to the proper game servers he should not be able to get the user to transmit the second authentication code without having allready transmitting the first one to the servers. And as soon as an authentication code has been used, it will never be accepted again. Neither will any previous codes, remember the codes are generated based on time and the servers should not accept codes in anything but chronological order. The adversary would not be able to acquire two, unused, chronologically created authentication codes.

There should exist, theoretically, a Man in the Middle tunnelling attack for the adversery to connect the user to the actual game servers, but through their own server. Passing along all game data between the server and the client and trying to, at some point, seize the connection and transfer it to his own full control. The user would be provided with an appropriate disconnect message and should the computer simultaniously get its network protocols or network connection get corrupted he would be unable to relog back in and hence unable to notify of any problem in time to stop anything.

The complexity of this is high of course. The game clients' code is not available and the clients change versions often. There's no API available and no easy way to gain knowledge of the communication syntax and protocols used between the game and server. It is complex, but absolutely possible.

Applying this scheme would obsolete the idea of having a dedicated authentication server, seperate from the gaming servers. The authentication process would have to be embedded into the game proper instead of in a lower level in the connection stack and this could prove to a big concern for some. Chosing to apply this security scheme could therefore add substantial additional cost and complexity to the game development. But it is, in my opinion, the only one that adds substantial security over the normal one-time codes and it should be considered regardless of its increased cost.

5.5 Games Have Complex Clients

Generally, in any information system, you want to avoid any security scheme that relies on its Security by Obfuscation. That is solely by confusing the adversary with a confusing system that he does not know the intricate secrets of. In the long run any adversary should be expected to be able to learn the system and its inner workings. The adopted law against this form of Security by Obfuscation is called Kerckhoffs Principle and was put forth by Auguste Kerckhoff [56] in the late 19th century. Plainly it states that you should be able to trust the security of your system even if your adversary knows the workings of your system. It should be secure even against its own creator.

Depending on Security by Obfuscation is like building a dam to keep a flood away from your house that you know is going to break at any time, you just wish that you will have moved by then. The three things that it does have going for it in the online gaming industry is that the game clients are very big and very complex, the limited life span of each individual game, and their developers dont have to share their proprietary code with anyone outside the development team.

If a gaming system becomes large or influential enough, then the investment of reverse engineering or cost of obtaining the necessary information about the system potentionally becomes worth it. But that cost should be very high. And there is nothingwrong with taking a few minor steps to further raise that cost. Many of these games actually have quiet a few game modifications released to them that the developers are not so happy about either. And raising the complexity of, and increasing the clients capabilities of detecting wether the game files have been modified helps battle these sorts of problems as well. These modifications included things ranging from changing your client-side representation of certain characters or modifying game sounds, to increasing your in-game running speed.

Ultimately the game developers don't want anyone to be able to modify their game files and, coincidentally, preventing the game files from being succesfully modified also increases security against adversaries exploiting a compromised user computer if the one-time codes are entered within the contexts of the game client as explained in last chapter on authenticating transactions.

6 Conclusion

As has been shown there is an actual security threat to online games. There exists tangible motives for attacking the online gaming industry and reports show an increasing occurrence of compromised gaming accounts. Account security is something that the online gaming industry must and, for the most part, is taking serious.

The wide variety of security schemes deployed across the industry may at first seem inefficent and confusing, but contrary to most other industries you might want to compare online gaming to their decisions on account security are made solely at their own discretion. They will, and should, chose the apropriate security scheme based on the product and their target audience.

Most game companies place the burden of making sure that their account is uncompromised solely on the user. Anything contained in or affiliated with the account is not the property of the user, but of the game company. The user only owns the right to use said account. The game companies can not be held responsible for anything lost due to the users negligent actions that caused the compromise of the account. Basically the only motive the game company has to alleviate their users concerns are to keep their customers happy and returning. With this in mind it is easy to see how the security of the accounts must be balanced against cost and system complexity.

A security scheme for an online game will only be viable if its cost of implementation is less than the lost revenue from potential security failures. And in contrast to most other comparable information systems this can be carefully balanced to maximze profit. Only the most popular and largest games, and the ones with sufficient adversarial motive, need to implement the most stringent security schemes. Being the smaller fish may prevent some games from being targetted and hence not require the more costly security.

However, the market for stealing gaming accounts is on the rise, and any game developer in todays climate of trojans and malware need to carefully consider what security scheme to chose. To rely solely on a username and password credential check means to invite anyone to gather information about your accounts and freely utilize these accounts for illicit or unwanted activities. Some form of two-factor authentication should be seriously considered for any and all game developers. It easily raises the level of effort needed to gain control of an account to what should be considered unfeasible for all but the most dedicated and motivated adversaries.

The demands and acceptance of the intended customers are probably what will eventually make the market converge on a well established standard for account security, but for now the differences are large. Understanding what the users are willing to accept in ways of cumbersome authentication schemes and providing them with cost-efficient yet effective ways to combat the growing security threat will be necessary in order to survive in the struggle for customers, and the battle against the malignant adversaries attempting to subterfuge the security of their accounts.

There are many forms of two-factor authentication schemes, some of which were covered earlier in this paper, but their main difference lies in their useability and their deployment cost. The choice of method should be based on the intended users preference and any presumptions that can be made about the target audience. *If at all possible, allowing the user to chose from a set of options will allow for the greatest flexibility.* Others might prefer a one-time pad or an authenticator chip, but I personally must say that I highly favour the use of an authentication code generating application on a smart phone because I have absolutely no problem with needing to keep my phone available at all times. The security of this application is nevertheless dependent upon the mobile device being physically seperate and untangled from any device used to perform the actual log-in.

The main conclusion of this paper is that there are a vast number of different choices that the gaming companies can make, and none of them are necessarily wrong. Depending on their threat level or the motives of possible adversaries the games might not even need to implement any Two-Factor Authentication, but it's my opinion that most should and will need to soon. When it comes to the choice of what delivery system to use this is a choice with more options than can be summarized in this conclusion, but the different options all have their own advantages and disadvantages based on their description in the previous chapters, or based on their nature of implementation regarding all the options that were not described. The popularity of the game and the size of the development budget and estimated revenue from the game should particularily be considered, but the demographic, habits and preferences of the game's audience should in my opinion be the most important. And this is probably the biggest difference, and the biggest advantage of the gaming industry when compared to other industries.

And at the highest level I believe the game developer should consider adding authentication within the confines of the game in a transaction authentication even if it should prove quite a lot more costly and complex.

No matter the soundness of the cryptographic protocols or the credibility of the chosen authentication scheme, if the users computer has been compromised then, in allmost all cases, all bets are off. A secure communication channel will not do much good if the end-point has been infected with malware targetting the product in question. At that point the only thing standing in the way of an adversary having complete access to your account is the complexity of sufficiently modifying the game files or taking advantage of the acquired information. An obstacle that will surely be overcome by the adversary at some time or another.

While the study of malware, the detection of it and preventing your computer from being infected byt it, is far beyond the scope of this paper it is an integral part of the security in online gaming. The term known as Defense-in-Depth properly describes what is necessary to prevent rampant infection of user computers; denying the adversary the oppurtunity to infect the computers by informing the users and customers of best practices in how to avoid getting infected. This is an enormous field in itself, but it is worth noting that game developers are presently actively informing their users about best-practices[20] as well as specific security threats in commonly used applications that need to be updated through their launcher applications or game forums, such as a warning from Blizzard published on their forum about a security hole in Adobe Flash for web browsers. [38]

Ultimately I believe that this is an exciting field that is still only in its early teens. I predict extensive further development will be necessary to keep up with an ever-increasing threat by ever-increasingly motivated adversaries in the coming years. However much I believe that this is a field in which the gaming companies could greatly benefit from consolidating their efforts and standardize a lot of the way they implement their account security, I'm expecting any large-scale combined effort is at least several years away. Also the process of developing legislative measures worldwide is a slow process and it will take even longer for it to mature to such a degree as to deter the continued and persistent efforts of malignant adversaries profiting off of any insufficiently secured assets.

References

[1] Interview with members of guild "'order of the white tiger"' from game server "'grim batol"'.

[2] Activision Blizzard. Vivendi and activision complete transaction to create activision blizzard. http://us.blizzard.com/en-us/company/press/pressreleases.html?080710. [Online; accessed feb 28th 2010].

[3] Activision Blizzard. World of warcraft surpasses 11 million subscribers worldwide. http://eu.blizzard.com/en-gb/company/press/pressreleases.html?081028. [Online; accessed feb 28th 2010].

[4] Alex Ziebart. Man in the middle attacks circumventing authenticators. http://www.wow.com/2010/02/28/man-in-the-middle-attacks-circumventing-authenticators/. [Online; accessed may 21th 2010].

[5] Christian Annesley. Banks tread warily over two-factor security. http://www.computerweekly.com/Articles/2006/03/28/215013/banks-tread-warily-over-two-factor-security.htm. [Online; accessed feb 20th 2010].

[6] Anonymous for Securology Blog. Targeted balk malware. http://securology.blogspot.com/2008/01/targeted-bank-malware.html. [Online; accessed may 21th 2010].

[7] Anonymous for www.geeks.co.uk. Activision's bobby kotick hates you. http://www.geeks.co.uk/7282-activision\%E2\%80\%99s-bobby-kotick-hates-developers-innovation-cheap-games-you. [Online; accessed may 30th 2010].

[8] Australian Institute of Criminoligy. Hacking motives. http://www.aic.gov.au/documents/1/B/A/\%7B1BA0F612-613A-494D-B6C5-06938FE8BB53\%7Dhtcb006.pdf. [Online; accessed March 20th 2010].

[9] "'account compromise info center"', community information on handling of compromised accounts. http://forums.worldofwarcraft.com/thread.html?topicId=3773308319. [Online; accessed may 16th 2010].

[10] Forum discussion between community representatives and funcom community manager. http://www.mmorpg.com/gamelist.cfm/game/191/view/forums/thread/276922/. [Online; accessed may 16th 2010].

[11] Ben Kuchera. Report: Mmorpgs revenues to explode over next few years. http://arstechnica.com/gaming/news/2007/09/report-mmorpgs-revenues-to-explode-over-next-few-years.ars. [Online; accessed feb 28th 2010].

[12] Benjamin Duranske. Two experts suggest virtual world profits may be taxable even before conversion to real world cash. http://virtuallyblind.com/2007/10/23/tax-virtual-profits-in-world/. [Online; accessed March 20th 2010].

[13] Beth Winegarner. Women's advocate, industry hero, sheri graner ray. http://www.gamespot.com/news/6120413.html. [Online; accessed March 20th 2010].

[14] bilingue, for kalibreonline.com. New virus attacks world of warcraft accounts with authenticators. http://kalibreonline.com/2010/03/01/new-virus-attacks-world-of-warcraft-accounts-with-authenticators/. [Online; accessed may 21th 2010].

[15] Blizzard Entertainment - Support Information. The negative impact of buying gold. http://www.worldofwarcraft.com/info/basics/antigold.html. [Online; accessed March 20th 2010].

[16] Charles Blazer. The five indica of virtual property. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962905. [Online; accessed feb 28th 2010].

[17] Cristina Jimenez . The high cost of playing warcraft. http://news.bbc.co.uk/2/hi/technology/7007026.stm. [Online; accessed feb 28th 2010].

[18] Daniel Terdiman. Congress to look into taxing virtual worlds. http://news.cnet.com/8301-10784_3-6126701-7.html. [Online; accessed March 20th 2010].

[19] Edward Castronova. Synthetic worlds: The business and culture of online games. Chicago:TheUniversityofChicagoPress..

[20] Eldariel, World of Warcraft Forum. [guide] protect your pc. http://forums.wow-europe.com/thread.html?topicId=273198555&sid=1. [Online; accessed june 15th 2010].

[21] Blizzard Enthertainment. Battle.net authenticator - blizzard. http://us.blizzard.com/store/details.xml?id=1100000822. [Online; accessed feb 20th 2010].

[22] IbisWorld. Video games industry research in us. http://www.ibisworld.com/industry/retail.aspx?indid=2003.

[23] A. Wiesmaier M. Fischer M. Lippert J. Buchmann. Outflanking and securely using the pin/tan-system. http://arxiv.org/abs/cs/0410025. [Online; accessed may 21th 2010].

[24] Jacqueline Carver. Dutch court rules virtual theft is real. http://static.rnw.nl/migratie/www.radionetherlands.nl/currentaffairs/region/netherlands/081022-virtual-theft-is-real-redirected. [Online; accessed March 20th 2010].

[25] Chris Hauck Jerry Felix. System security: A hacker's perspective, 1987.

[26] Julian Dibbell. The decline and fall of an ultra rich online gaming empire. http://www.wired.com/gaming/virtualworlds/magazine/16-12/ff_ige?currentPage=all. [Online; accessed feb 28th 2010].

[27] Brian Krebs. Citibank phish spoofs 2-factor authentication. http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html. [Online; accessed may 21th 2010].

[28] John Leyden. Warcraft gamers locked out after trojan attack. http://www.theregister.co.uk/2006/09/29/warcraft_trojan_attack/. [Online; accessed may 16th 2010].

[29] Liam O Murchu. Banking in silence. http://www.symantec.com/connect/blogs/banking-silence. [Online; accessed may 21th 2010].

[30] Liam O Murchu. Trojan.silentbanker. http://www.symantec.com/security_response/writeup.jsp?docid=2007-121718-1009-99. [Online; accessed may 21th 2010].

[31] Marcus Yam. Ea mandates online, dlc for every game in 2011. http://www.tomsguide.com/us/mass-effect-dragon-age-online,news-5781.html. [Online; accessed feb 28th 2010].

[32] Mark Ward. Does virtual crime need real justice? http://news.bbc.co.uk/2/hi/technology/3138456.stm. [Online; accessed March 20th 2010].

[33] 'Martin' for www.ghacks.net. Ubisoft to introduce online copy protection for pc games. http://www.ghacks.net/2010/02/20/ubisoft-to-introduce-online-copy-protection-for-pc-games/. [Online; accessed feb 28th 2010].

[34] Matthew Yi. Stacks of new releases for ... http://www.sfgate.com/cgi-bin/article.cgi?f=/chronicle/archive/2004/12/18/MNGUOAE36I1.DTL. [Online; accessed feb 28th 2010].

[35] Mike Masnick. Nice work retrieving that magic sword... but now you need to pay uncle sam for it. http://www.techdirt.com/articles/20061017/163943.shtml. [Online; accessed March 20th 2010].

[36] Murad Ahmed. Avatar identity theft: Police in britain make an arrest. http://www.futurecrimes.com/virtual-world-crime/avatar-identity-theft-police-in-britain-make-an-arrest/. [Online; accessed March 20th 2010].

[37] N/A. Virtual economies. http://www.virtualeconomies.net/. [Online; accessed feb 28th 2010].

[38] Nethaera, Blizzard employee . Security alert - adobe flash, reader, acrobat. http://forums.worldofwarcraft.com/thread.html?topicId=6864486401. [Online; accessed june 15th 2010].

[39] United States Department of Agriculture. Homeland security presidential directive 12. http://hspd12.usda.gov. [Online; accessed feb 20th 2010].

[40] Piers Harding-Rolls. Western world mmog market: 2006 review and forecasts to 2011. http://www.screendigest.com/reports/07westworldmmog/pdf/SD-07-03-WesternWorldMMOGMarket/view.html. [Online; Accessed March 20th 2010].

[41] Andres Sehr Press Release. Spotify security notice. http://www.spotify.com/no/blog/archives/2009/03/04/spotify-security-notice. [Online; accessed may 16th 2010].

[42] Blizzard Entertainment Press Release. Battle.net mobile authenticator for android mobile devices. http://us.blizzard.com/en-us/news/?d=2010-2#101500. [Online; accessed may 21th 2010].

[43] Blizzard Entertainment Press Release. Battle.net mobile authenticator now available on apple app store. http://us.blizzard.com/en-us/news/?d=2009-3. [Online; accessed may 21th 2010].

[44] Press Release. Skandiabanken fjerner sertifikatet. http://www.skandiabanken.no/SKBWEB/VisNyheter/6/21630/SKBWEB/Oss/Presse/Pressemeldinger2010.aspx. [Online; accessed may 16th 2010].

[45] Bruce Schneier. The failure of two-factor authentication. http://www.schneier.com/essay-083.html. [Online; accessed may 21th 2010].

[46] Sachin Shetty. Introduction to spyware keyloggers. http://www.symantec.com/connect/articles/introduction-spyware-keyloggers#ref1. [Online; accessed may 16th 2010].

[47] Sophos. Drive-by downloads remain cybercriminals' favorite web threats. http://www.sophos.com/pressoffice/news/articles/2007/08/toptenjul07.html. [Online; accessed may 16th 2010].

[48] Michael Stutz. Aol: A cracker's paradise? http://wired-vig.wired.com/science/discoveries/news/1998/01/9932. [Online; accessed may 16th 2010].

[49] Symantec. Symantec internet security threat report march 2007. http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf. [Online; accessed june 15th 2010].

[50] Iain Thomson. Microsoft to abandon passwords. http://www.v3.co.uk/vnunet/news/2126966/microsoft-abandon-passwords. [Online; accessed may 21th 2010].

[51] Tyren, Blizzard representative. Forum announcement: Blizzard authenticator currently sold out. http://forums.worldofwarcraft.com/thread.html?topicId=7475467221&sid=1. [Online; accessed may 5th 2010].

[52] Uncredited for BBC News. "'game theft"' led to fatal attack. http://news.bbc.co.uk/2/hi/technology/4397159.stm. [Online; accessed March 20th 2010].

[53] Urizeus Sklar. Top second life entrepeneur cashing out us$1.7 million yearly. http://nwn.blogs.com/nwn/2009/03/million.html. [Online; accessed feb 28th 2010].

[54] Wagner James Au. Who wants to be a virtual world millionaire? http://gigaom.com/2006/11/29/anshe-chung/. [Online; accessed feb 28th 2010].

[55] Wikipedia. Altinn. http://no.wikipedia.org/wiki/Altinn. [Online; accessed june 15th 2010].

[56] Wikipedia. Auguste kerckhoff. http://en.wikipedia.org/wiki/Auguste_Kerckhoffs. [Online; accessed june 15th 2010].

[57] Wikipedia. Blizzard entertainment. http://en.wikipedia.org/wiki/Blizzard_Entertainment. [Online; accessed feb 20th 2010].

[58] Wikipedia. Botnet. http://en.wikipedia.org/wiki/Botnet. [Online; accessed feb 20th 2010].

[59] Wikipedia. Certificate authority. http://en.wikipedia.org/wiki/Certificate_authority. [Online; accessed may 16th 2010].

[60] Wikipedia. Everquest. http://en.wikipedia.org/wiki/Everquest. [Online; accessed feb 28th 2010].

[61] Wikipedia. Farmville. http://en.wikipedia.org/wiki/FarmVille/. [Online; accessed feb 28th 2010].

[62] Wikipedia. Phishing. http://en.wikipedia.org/wiki/Phishing. [Online; accessed feb 20th 2010].

[63] Wikipedia. Public key infrastructure. http://en.wikipedia.org/wiki/Public_key_infrastructure. [Online; accessed may 16th 2010].

[64] Wikipedia. Ultima online. http://en.wikipedia.org/wiki/Ultima_online. [Online; accessed feb 20th 2010].

[65] Wikipedia. Ultima online. http://en.wikipedia.org/wiki/MUD. [Online; accessed feb 28th 2010].

[66] Zarakiteque, World of Warcraft Forum. Hacked with authenticator. http://forums.wow-europe.com/thread.html?topicId=12730404058&sid=1. [Online; accessed may 21th 2010].