Game Consoles - Are they secure?

Halvar Myrmo

Master's Thesis
Master of Science in Information Security
30 ECTS
Faculty of Computer Science and Media Technology
Gjøvik University College, 2007

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Faculty of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

The new game consoles and handheld machines available on the market today are designed with Internet and multiplayer connectivity in mind. They are also designed to be used for several years to come, and to be connected to the Internet 24 hours a day. This combination of computational power and connectivity could make the game consoles lucrative targets for viruses, Trojans, botnets, spam and other malware.

Users of home computers are slowly learning that they need to protect their computers through the use of firewalls, antivirus and the like. But most of us probably do not consider a game console to be a computer, and therefore does not consider protecting it the same way we protect a normal computer.

The goal of this thesis is to find out if new vulnerabilities are introduced into the home when connecting a gaming console to the Internet. We also take a look at children's use of computer and video games, and what the parents know about it. We try to combine this information into an overview of how secure it is to use a game console and play computer and video games online.

Sammendrag

De nye spillkonsollene og håndholdte maskinene som finnes på markedet i dag er designet med tanke på Internett og flerspiller muligheter. De er også designet for å vare i mange år og for å være koblet til Internett 24 timer i døgnet. Denne kombinasjonen av regnekraft og tilkoblingsmuligheter kan gjøre spillkonsoller ett lukrativt mål for virus, trojanere, botnet, spam og annen ondsinnet programvare.

Eiere av datamaskiner begynner sakte men sikkert å lære at de trenger å beskytte datamaskinen sin med brannmur, antivirus og lignende. Men de fleste av oss anser nok ikke en spillkonsoll for å være en datamaskin, og vil derfor ikke tenke på å beskytte den på samme måte som en vanlig datamaskin.

Målet med denne oppgaven er å finne ut om det introduseres nye sårbarheter i hjemmet når en spillkonsoll kobles til Internett. Vi tar også en nærmere kikk på barns bruk av data og videospill, og hva foreldre vet om dette. Vi prøve å sammenfatte denne informasjonen til ett helhetlig bilde over hvor trygt det er å bruke en spillkonsoll og spill data og videospill på Internett.

Contents

List of Figures

List of Tables

List of Definitions

- **Hacker**: Hacker is used to describe a person who is an expert or enthusiast of any kind. It is often used to describe person who have proven to be exceedingly good at programming, or one who is able to program fast.
- **Cracker**: A cracker is a person who uses his or hers skills to break security measures in software and hardware.
- **Modified**: When used in conjunction with a game console it means that the console has been altered in some way to be able too perform tasks that the creators didn't intend.
- **Modification chip**: Often called modchip. This is devices that are added to a game console in order to make it perform tasks other than ones originally intended by the creators. This involves playing backed up, imported and homebrewed games and/or to circumvent the digital rights management systems of the game console.
- **Game Console**: A dedicated device used to play video games. It can either be connected to a TV or other screen output, or it can have its own built in screen.
- **Homebrew**: Homebrew, referred to in the context of games and game consoles, is the creation of software or games by the consumers.
- **Transmission Control Protocol**: Transmission Control Protocol (TCP) is a connection based transmission protocol that is one of the core protocols used on the Internet. The protocol guarantees such services as reliability and delivery in the correct order.
- **User Datagram Protocol**: User Datagram Protocol (UDP) is a connectionless based transmission protocol much used on the Internet. It gives none of the guarantees that TCP does, but instead uses a best effort approach. It is mostly used by applications that don't need guaranteed delivery of traffic.
- **Botnet**: Botnet is a term used to describe a collection of software robots that is interconnected through a network. In the most common use of the word it means a collection of computers that has been taken over by a cracker, and is used to help the cracker. This can be to send spam mail, run Denial of Service attacks and so on.

Preface

This master thesis is my final work after two years of master thesis studies at Gjøvik University College. I have been playing computer and video games for years, and when the opportunity to write a master thesis that combined information security and gaming arose, I jumped at it.

I would like to thank my supervisors, Frode Volden and Espen Torseth. Without them I would probably have faltered sometime during the project. I would like to thank the Norwegian Centre for Information Security (NorSIS) for providing funds in order to get some of the hardware needed for the project.

Thanks also to my brother, and again Espen Torseth, for lending me their privately owned game consoles. Without these I wouldn't have been able to test as many consoles as I did.

And I would like to give thanks to all the people who answered my survey, without them I would never have finished the work.

June 30 2007
Halvar Myrmo

1 Introduction

1.1 Chapter summary

This chapter gives a brief introduction into the topic of this paper. First we give a short introduction with a problem description. We look at the motivation behind the project, and list the research questions. Then we give a summary of claimed contributions and at the end of the chapter we give a brief outline of this document.

1.2 Topic

The modern game console of today is no longer exclusively designed to play games. They are very powerful computers, often the most powerful computer in a household. And the number of services that can be run on a game console is ever increasing. We still have the old functionality of online gaming, score keeping, gamer profiles, ranking systems, clans and so on. But a modern game console often offers other services as well, such as Internet browsing, instant messaging, movie playback, streaming of content from a computer and much more. As the game consoles become more powerful and more complex they also become more vulnerable to network based attacks.

But there is also a concern about children's protection of privacy. Children today are often taught how to behave when using the Internet. They learn what information they should protect, what they should do if they come across something they don't know, who they should and shouldn't talk to and so on. But when it comes to a game world, which is specifically designed to be all fun and games, are these lessons still remembered? Or are they even taught to the children within this context?

Keywords: Nintendo Wii, Xbox, PlayStation, game consoles, security, network, protection of privacy.

1.3 Problem description

The seventh generation of game consoles are a giant leap forward in computing power, connectivity and availability compared to the sixth generation. As the game consoles become more powerful and the software more complex, this opens up for more unknown vulnerabilities. And since there are millions of units out there, it might be a potential target for crackers. The PlayStation 2 alone sold over 100 million units. Security related topics are something the computer world has struggled with for decades, and it would be a good idea that the manufacturers of game consoles consider this as early as possible. We will take a look at several game consoles, and see what kind of security measures that they have implemented.

At the same time there are other concerns about security when discussing game consoles and games. A game world or a virtual world often revolves around a concept of having fun. This is often the main purpose of such a world; it is an advanced toy. But this could also mean that users of such toys will forget that the same rules of personal privacy protection that applies to everything we do on the Internet, also should apply in a virtual world. We will try to determine how people view virtual worlds, and how they protect their personal information in such places.

1.4 Motivation

Expressions like computer viruses, self-propagating worms, Trojan horses, backdoors, vulnerabilities, exploits, botnets and so on, are well know in the computer world. They are also slowly emerging on the cellular phone platforms. The next step in this evolution might be game consoles. More and more of them are being connected to the Internet, and this might open up for new and unforeseen consequences. By starting the work early, and using the lessons learned in the computer world, we might be able to get a jump start on these potential problems.

1.5 Research questions

1. Does the installation of a new game console in the home open for new vulnerabilities that we are not aware of?
2. Are there more potential vulnerabilities in a console that has been modified, than in an unmodified console?
3. Do we need to take special precautions when connecting a new game console to the home network?
4. Does users of game and virtual worlds consider their privacy protection in the same way they do when using other services on the Internet?

1.6 Summary of claimed contributions

There is a lack of research in the area of security in game consoles. It has not received a lot of attention from the academic community over the years. This is understandable since they have traditionally posed no major threats, but with the later years developments this has changed. Game consoles are becoming increasingly connected to the Internet, and the number of units sold is growing.

We have tried to make a broad overview of many game consoles, both normal consoles and handheld ones. Using these consoles we have conducted several technical experiments, trying to see how they react to different types of manipulation. To balance these technical experiments, we conducted a survey amongst parents with children in grade school. We wanted to find out how parents relate to game consoles, how children are taught netiquette, if they have considered security in regards to game consoles and game worlds, and much more.

1.7 Outline of the report

Chapter 2: This chapter gives some background information from areas of research that is interesting in regards to this topic.

Chapter 3: Chapter 3 explains the methods we choose to use during this project. We explain why we have done it the way we have, and what choices was made during the project period.

Chapter 4: This chapter gives an introduction to the equipment, software and hardware we have used during this project. There is a brief overview of each game console in question, and some of the software used.

Chapter 5: Chapter 5 contains the results we got from the technical experiments. We look at all the consoles that we have tested, and present the results we have from each.

Chapter 6: This chapter contains the results we got from the analysis of the statistical material we gathered through our survey.

Chapter 7: In chapter 7 we present a discussion of our results. After the discussion we try to draw some conclusions based on the results and the discussion.

Chapter 8: During the project period we came up with a lot of new ideas and questions. These are presented in chapter 8.

2 Related work

2.1 Chapter summary

This chapter looks at different areas of interest to this project. There is little, if no, directly related work to security in game consoles, so we look to different areas of interest to try and find perspectives and information than can be useful. We take a closer look at how the modification community works, what we can learn from the computer world, how rootkits work, some information on distributed computing and botnets, cheating in games, homebrew software and some information about child grooming.

2.2 The modification community

A modification chip, or modchip, is a device that enables a gaming console to perform tasks that it was not originally designed to do. This includes the running of imported, backed up, downloaded and homemade software. In some cases it also tries to circumvent the traditional Digital Rights Management systems incorporated into many consoles. A large community of users and developers has sprung up around these modchips, and a lot of homemade software can be found. The game console that can be said to be the most exploited in this sense is the original Xbox [1]. This gaming console developed by Microsoft [2] resembles a generic computer in many ways, and therefore have been very popular in the modification community because of how easy it has become to modify. But it also exists modchips to a lot of other consoles, e.g. the original PlayStation [3], Sega Saturn, Sega Dreamcast, PlayStation 2 [3] and Nintendo GameCube [4].

Although there exists modchips to a lot of different game consoles, the largest modification community circles around the Xbox [5] since this console has proven to be the easiest to modify. The people working on the Xbox Linux project [6], trying to run Linux on an unmodified Xbox, has released a document describing 17 mistakes Microsoft made in the design of the Xbox security system [7]. A modified Xbox can be made to do a lot of things that the developers never intended. The original dashboard can be swapped for a new one, homemade software can be run, FTP services can be used to upload or download material to and from the Xbox, backed up or pirated games can be run, larger hard drives can be installed and it is also possible to run full instances of Linux. This proves that a lot can be done to the original hardware to circumvent protection measures, and therefore it could also be possible to use this hardware for other purposes, for instance a dedicated gaming console that sends out spam. Vaughan [8] gives us a comprehensive look at how to treat a modified Xbox as forensic evidence, and different forensic recovery methods that can be used on a modified Xbox. [9], [10] and [11] all gives very comprehensive insight into how we can alter our game console and make it into something altogether new. All these alterations might also open for new and unforeseen vulnerabilities in the game consoles.

2.3 Lessons learned from the computer world

Defending against malicious software and network attacks is something the computer world has been doing for decades now and therefore it is logical to look for solutions to these potential problems in the computer world. Sources like [12, 13, 14, 15, 16, 17] can give us a comprehensive insight into various areas of computer and network security.

Computer security revolves round the research, tools, hardware, software and administrative work of securing computers in such a way that we can use them without voiding a given policy. This field has been in development for several decades now, and are still growing. By applying the lessons learned from this field on gaming consoles and consumers goods in general, a lot of vulnerabilities can be mitigated from the very start.

The term host hardening describes "taking a typical or default installation of an operating system or application and making modifications to decrease the potential exposure to threats [17]". This also applies to game consoles, in more ways than one. The developers of game consoles usually focuses on Digital Rights Management and making sure that their console cannot be used to execute software or games that they have not given permission. Several techniques is used to ensure this, e.g. in the original Xbox "executables (.xbe files) are encrypted with 2048 bit RSA security [8]". These kinds of security measures means that the developers of modchips described in 2.2 cannot break the security, they rather looks for ways to circumvent it, trying to find loopholes in the security that the developers didn't think of.

Another reason why game console developers use much time to make sure that the DRM of their systems are unbreakable is the fact that consoles often are sold with a loss. Both the original and the new Xbox are sold with loss [18], and according to iSuppli [19] Sony loses as much as over $300 per sold PlayStation 3. The reason for this is that the companies making and selling these consoles wish to make the hardware itself obtainable, and then make money on the software, games and accessories sold. Therefore it is crucial that it is difficult if not impossible to play copied or homemade games and software on the console.

But another part of the host hardening that the developers should be aware of is the potential for malicious software run on their consoles. We only need to look at the work of Chris Vaughan [8] in order to see that law enforcement agencies and forensic experts already recognises the potential for using the Xbox for a lot more than just playing copied games. This could also be possible with the new consoles being released. The new consoles released in today's market are all designed with Internet connectivity in mind, and the software that they run are becoming ever increasingly more complex. This leads too an increase in potential vulnerabilities that should be taken seriously.

2.4 Rootkits

The ultimate goal any attacker is the possibility to install a rootkit onto a compromised machine. A rootkit is

> a set of programs and code that allows a permanent or consistent, undetectable presence on a computer. [20]

The word rootkit comes from the fact that this set of programs and code allows an attacker to maintain access to the root or administrative account on the computer in question. It is used to hide running processes, files, folders, remotely controlling the computer and giving it commands, sniffing network traffic, shutting down other security measures and generally turning the compromised computer into a zombie that is always ready to act on the behalf of the attacker.

A rootkit is not inherently a "bad" thing; it is a technology that can be used for several purposes. Law enforcement agencies might use a rootkit in a lawfully sanctioned operation, militaries might use it as a weapon in war and large corporations might use rootkits to monitor that their policies are being followed. Some software is also using rootkits, or similar techniques, to avoid detection or tampering. Examples of such software are Alcohol 120% and DAEMON Tools. Both these are disk image emulators that make it possible to run images of CDs and DVDs as virtual disks directly from the hard drive. They are often used to mount downloaded games and movies, and therefore some of the Digital Rights Management systems that exists will check the computer that it is about to be installed on and if it finds instances of this software will either deny installation or even uninstall the software. As a consequence of this DAEMON Tools altered their software so that driver names, drive-vendors and version numbers were randomly generated [21].

Rootkits can be exceedingly sophisticated in the way they operate, and there is several ways that they deploy themselves. One of the more common types is the kernel level rootkit. This type of rootkit infects the kernel of the operating system, usually through a device driver or some other loadable module. Kernel level rootkits can be very difficult to detect and remove, since they often alter large parts of the operating system in order to hide themselves. Another common type of rootkit is the library level rootkit. These rootkits patch, hook or replace system calls with information that hides the existence of the rootkit. Hooking is a technique where the rootkit takes over at start-up of a program or procedure and runs itself instead. After it is finished it jumps back to the normal execution, thus creating a hook in which the rootkit always takes precedence over the regular execution.

Hooking also applies to application level rootkits. An application level rootkit is a normal user application in which the normal execution of the code has been altered in some way. It can be hooks, patches, an entirely faked program, injected code and much more.

The lowest level of rootkits to date is the virtual machine based rootkit. A virtual machine is

> an abstraction layer that decouples the physical hardware from the operating system to deliver greater IT resource utilization and flexibility.
>
> *VMware.*

This makes it possible to run operating systems on an abstract machine. Some virtual machines also make it possible to run several operating systems at the same time, completely separate from each other. A virtual machine based rootkit is a rootkit that acts as a virtual machine. Upon start-up of the machine, the rootkit loads itself and then it loads the guest operating system as a virtual operating system without the knowledge of the end user. This type of rootkit requires that the attacker is able to compromise a system and get sufficient access to alter the boot sequence. A proof of concept virtual machine based rootkit called "SubVirt" was developed jointly by the University of Michigan and Microsoft Research. [22]

The rootkits that are most applicable to game console are probably the firmware level rootkits. Firmware is used to denote software that runs on dedicated hardware, such as mobile phones, routers and game consoles. In the seventh generation of game consoles all major manufacturers has enabled their systems to update the firmware over the Internet. But is has been proven that such firmware can also be infected with rootkits, and therefore the game console manufacturers should take some precautions in order to protect the firmware of game consoles.

2.5 Distributed computing

With the introduction of the PlayStation 3 (see section 4.2.2) into the seventh generation of game consoles, the computing power of a modern game console has taken a huge leap forward. The central processing unit of the PS3 is the Cell microprocessor, created jointly by Sony, Toshiba and IBM. Cell is used as shorthand for Cell Broadband Engine Architecture. The Cell microprocessor consists of one high performance PowerPC based CPU called the Power Processing Element (PPE) which in turn controls eight co-processors called Synergistic Processing Elements (SPEs). All of these SPEs runs at 3.2 GHz. Six is always readily available for the PPE to use, the seventh is reserved for the operating system and security, while the eight is disabled in order to improve the production yield. It also has an Element Interconnect Bus (EIB) used to connect the different elements on the chip. Using this setup, the Cell processor is able to achieve "204,8 Gflop/s, with a computational intensity of 32 FLOPs/word" [23], which is a lot more than the standard desktop computer is able to output.

This makes the Cell processor, and therefore the PlayStation 3, a good choice when building distributed computing networks. This has also been proven with the PS3. It is possible to connect it to the Folding@home distributed computing project [24], which uses computing power from people all over the world to

> understand protein folding, misfolding, and related diseases.

For this to work, the project needs a lot of computing power. This has been arranged in such a way that people can download a client to their computer, or PlayStation 3, and solve a small part of the problem. This part is uploaded to the project via the Internet, and the computer can be used to solve another small part of the problem. With enough participants it is possible to solve huge mathematical problems this way.

As mentioned before, it is possible to connect a PlayStation 3 to this project. Half a year after the release of the PS3 in the US, the PS3s connected to the project has completely taken over the performance charts. The few PS3s, compared to the number of regular computers, connected to the project put out a huge amount of terra flops. Micrsoft has also said that they are looking for similar applicatinos for their Xbox 360 [25]. This shows that today's modern game consoles have a lot more areas of use than the game consoles of the previous generation. But this computing power could also be used for "bad" purposes, e.g. brute forcing encryption keys.

2.6 Botnets

The next logical step from distributed computing and grid networks, from a crackers perspective, is botnets. The term botnet can be used about any group of automated computers that work together against a common goal, but it usually describes networks of computers that are used for a different purpose. In the most common use of the word, a botnet is a collection of computers that a cracker has somehow taken control over and is using for some purpose or other. The owner or user of the computer rarely knows what has happened. The person creating such a net can collectively call upon all the computers in the network, and make them do some task. Such tasks might be to run denial-of-service attacks, or send adware or spam and so on. With the large amount of game consoles sold today, and more and more of them coming online, the possibility of game consoles becoming part of a botnet is no longer as unlikely as it was five years ago.

2.7 Cheating in games

Video games have been around for a long time now. Some of the first games emerged around the end of the 1940's, and since then have developed into massive games where hundreds of thousands of users can play at the same time. This massive expansion of video games also comes with a darker side to it, people who cheat. In the early decades of video games this was not a big problem, since cheating only would occur on a local level and only affect the one user playing a that location. In fact many game manufacturers incorporated cheats into their games, so that players that for some reason couldn't or wouldn't play within the normal rules could cheat their way through the game. Some common cheats are to become invulnerable, often called "God Mode", giving yourself infinite resources, invisibility, removing obstacles, etc.

But with the emergence of multiplayer games and Internet, cheating became a serious problem. It is no fun for the players when the ones they play against can cheat and make themselves and their performance reach levels unobtainable by normal human interaction. This can lead to new players just abandoning the game, without really trying, getting fed up with loosing all the time. Cheating can kill a good gaming community. Therefore many game developers are implementing anti-cheat measures into their games. But creative crackers with a lot of time on their hands often find ways around these measures.

One good example of this comes from the world of Quake. This was one of the first major hits in the world of online gaming, and this lead to a lot of gamers joining up. The game was originally released in June 1996, and the source code was made open source under the General Public License (GPL) in 1999. Soon after this cheats for online playing started appearing on the Internet. In an unpublished Internet article [26] Raymond takes a look at these newly discovered cheats, and discusses how to mitigate them. It is also discovered that the cheats, thought of as fairly new, had been around from long before the source code had been made public.

There are several different security issues in online games. Yan et al. [27] started building a taxonomy of online cheating, and further elaborated on this in [28] by using online bridge as an example game. Smed et al. took a closer look at the networking aspects of online gaming [29], and later elaborated on the same subject [30]. We will only be taking a brief look at some these findings:

1. **Escaping, disconnecting**
   Escaping or disconnecting is a way of cheating where a player that knows he or she is going to loose the game, quits before it is finished. This means that the game will not be marked as a loss in that players game statistics, and doing this makes it possible for a player to get ranked very high without any losses tied to his or hers gaming account. There is several ways to battle this type of cheating. The popular online game StarCraft from Blizzard has statistics over how many times a player has disconnect from a game session, so that other gamers can use this information to

decide if they want to play against that player [27].

2. **Farming**
   Farming is an expression used about selling virtual assets in the real world for real money. This often involves a player, or an automated player called a bot, collecting, or farming, a lot of resources in a virtual world. Then these virtual resources are sold in the real world, e.g. on IGE [31], for real money, to other players in the game. This is by many considered cheating, but by others considered as a way of getting ahead in a virtual world. One of the most prominent examples of this practise comes from the game World of Warcraft, where there has been reported as many as a hundred thousand Chinese gamers having farming as a regular job [32].
   There has been some controversy surrounding the topic of farming. Some players say that the practise might bring jobs to people who otherwise might not have a job, and this way create jobs and income. They also argue that players who enter the virtual world long after the first players have a hard task ahead of them, trying to catch up with the more experienced players. Using the benefits of farming, they can then pay their way to the top, without having to spend a lot of time getting to the level of other players. Other players argue that this practise violates some of the principle of virtual games and virtual worlds. The people not willing to participate in this practise has to spend that much more time in the virtual world to be able to keep up with the players willing to pay their way to the top. They also argue that this practise can harm the economic balance in the virtual world.
   Game developers have been known to look down upon the practice of farming, and in many cases it is actually explicitly denied in the EULA of the game. Players that have been caught in this practice often get their game account banned from the game.

3. **Denial of Service cheating**
   Denial of Service cheating comes in several forms. One way to do this is to try and log into an account with a known username [27]. Such usernames are often revealed in the game world. If there is a player that someone wants to block from the game for a period of time, he or she can try multiple login attempts with that account ID. Some systems will then, in order to battle brute force login attempts, only allow a given number of login attempts before the account is disabled for a time. This means that this player is effectively banned from the game for a period.
   Another way of using Denial of Service to cheat in games is to monitor the traffic flow to and from the computer used during game play, often with a packet sniffer like Wireshark [33]. When the IP address of the opponent is discovered, a real life Denial of Service attack can be launched. This can be seen as a means to avoid loosing a game, forcing the opponents' connection to the Internet to slow down so much that the game does not function properly.

4. **Eavesdropping game traffic, traffic tampering, reflex augmentation**
   This kind of cheating demands a lot of preparation, some quite sophisticated software and probably an extra machine that can act as a proxy. The player wanting to use this type of cheating has to set up another machine between the machine used for gaming, and the Internet. This machine acts as a router, as well as a packet sniffer. This is done because many new games has methods of detecting whether or not the machine used for playing has software used for cheating running. When the proxy is up and running

it can be used to eavesdrop on the communication between the players, and possibly glean information from this traffic that he or she should not have access to.
This information could also be used for reflex augmentation [29]. The proxy can sniff the traffic and keep track of where the other players are, giving the cheater unfair advantages. The cheater can also use the proxy to enhance the performance of the playing. E.g. when firing a weapon, the proxy can add information to the information stream making the aim more accurate. This can also work the other way around. The proxy can stop the data packets that tells the game that the player has been hit, thus making the player invulnerable.

5. **Modifying software, game data and hardware**
   Modifying the game data, software running on the computer or the hardware itself can also be used to cheat in games. Modified graphic card drivers could make it possible to see through walls. A cracked game client could make it possible to see hidden information like the status of the other players [29]. Games that base their security in some hardware can feel the effects of cheating if ways to modify the hardware itself are found.

6. **Exploiting bugs or design flaws**
   Cheating by exploiting bugs or design flaws in games is quite common in the gaming world. On classic example found in the world of first person shooters (FPS) are "bunny hopping". The bunny hopping is a trick performed while jumping in the game. When in the air the player turns right, while at the same time strafing in the same direction of the turn. At the exact time of landing, the player jumps again avoiding the built-in deceleration that happens when hitting the ground. By using this method consecutively for a period of time the player might accelerate to speeds far greater than originally intended by the game developers.
   This type of cheating can often be mitigated or removed by doing patching and firmware updates of the games.

The problem with cheating in virtual worlds and games are one that should be taken seriously, especially when the possibility of making real world money in the game comes into question. As seen with farming, it is possible to make money in a game world. Microsoft ran an Xbox rewards competition from February 12. 2007 making it possible to win real world goods and gadgets [34]. In the virtual world Second Life [35] it is possible to make virtual money, and then cashing them out in real life money on a later stage.

> The emergence of online games fundamentally changed the security requirement for computer games. In the new context, copy protection is not, at least not the only, security issue any more. [27]

Several attempts have been made by the academic community to mitigate cheating in online games. Chambers et al. attempted to create a protocol that would not prevent cheating, but rather detect it after a game of Real Time Strategy was completed [36]. When a cheater is detected that players account can be banned from the system. DeLap et al. applied runtime verification to centralised online games with some success [37].

2.8 Homebrew

Homebrew is the creation of software and/or games by the consumers. One of the advantages that game console developers have is that they can control the software that runs on their hardware. Unless the owner of the hardware modifies the game console, it is usually impossible to run his or hers own code. This is a great security advantage, since untrustworthy code cannot run on the hardware.

But with the emerging online services like YouTube and Facebook, user generated content is becoming increasingly popular. At the same time the expenses for creating games is on the rise. As a result of this, the major game console developers are opening up their consoles to more homebrew software.

Microsoft's has released a free Software Development Kit (SDK) as part of their XNA Game Studio series of development tools [38]. There are two SDKs in this series, the XNA Game Studio Professional and the XNA Game Studio Express. The professional version targets itself towards professional game developers. The express version is free, and targets itself against students, enthusiasts and homebrew developers. The free kit can be used to create and run computers games on the Windows platform. When creating games for the Xbox 360 the developer has to subscribe to the XNA Creators Club. This cost a small annual fee.

The PlayStation 3 was designed to be able to run other operating systems from day one. The most popular operating system has been Linux, and several different distributions have been tested on the PlayStation 3. Through Linux, homebrew developers have access to much of the PS3 hardware. There is limited access to the graphics subsystems at the time of writing, but the graphics manufacturer Nvidia is known for making good Linux drivers for its hardware. It is expected that this also will be the case for the PS3.

Many of the professional game development kits available today are often very expensive. This often leads to the fact that smaller game developers and homebrew developers cannot afford the kits. Nintendo has taken this under serious consideration, and are releasing a cheaper and more lightweight game development kit [39]. This system, called WiiWare was launched late June 2007 and is aimed at making game creation more accessible for small and independent game developers [40].

The most problematic issues with homebrew software are security related. Allowing anybody to create software to be run on the game consoles opens up a whole new world of potential problems. Both Microsoft and Sony have solved this through the use of a hypervisor. In earlier game consoles, when a game was started it took over the console completely. With a hypervisor approach, the operating system of the game console never releases control of the hardware. All system calls has to go through this hypervisor, and Microsoft and Sony seems to be confident that this approach might mitigate potential vulnerabilities. All they have to do is to harden the hypervisor to make sure it does not contain any security related vulnerabilities. But it has been discovered that the hypervisor running on the Xbox 360 contained a locally exploitable vulnerability, making it possible to run unsigned code [41].

2.9 Child grooming

The expression child grooming can be used in more than one context, but for our purposes we are talking about a deliberate act by an adult in preparation of sexual abuse of a child. This preparation can be many things, but it always involves gaining the child's trust in some way. The usage of Internet is known to be popular in grooming. Using chat rooms, web forums, instant messaging and so on, to get to know children and eventually meet them in person.

The usage of game worlds for this purpose might pose new problems for children and parents. Teaching children netiquette can help mitigate the potential risks with child grooming, and teaching children what is safe and what is not safe online might help. But child grooming in the context of computer and video games played online is a somewhat different problem. These arenas are considered fun and game, and might not be taken as seriously as chatting or surfing the web. A child might not consider that when playing online we are essentially in the exact same position as when chatting online, only the setting has changed.

It has been suggested that the built-in PictoChat function in the Nintendo DS can be used as a child molestation tool [42]. It is not known how much used the PictoChat function is. But with Nintendo DS hotspots being created all over the world, this might be a serious concern. Nintendo also warns about this possibility in the Nintendo DS manual:

> To protect your privacy, do not give out personal information such as last name, phone number, age, e-mail or home address when communicating with others. An adult should assist children with system setup and instruct them not to use personal information. Children should be warned about communicating with or meeting strangers.

3 Choice of methods

3.1 Chapter summary

The choice of method [43] is based on the pre-project of the master thesis. We describe the different approaches to the problem that we considered. We then present some information on how the technical experiments and the survey were conducted.

3.2 Our choice of method

In the process of developing the foundation for this thesis we considered several ways of approaching the problem. The title of the thesis is "Game consoles - are they secure?". What do we mean by secure? Security can have several different meanings. We decided that in our context security should be from the user's point of view. What measures do the manufacturers of game consoles take to protect their customers? What does the users of video games, computer games and game consoles do to protect themselves?

We decide early on that we wanted to conduct some purely technical experiments. We wanted to do this to see what security measures the manufacturers of game consoles use. These measures are usually not advertised or even discussed anywhere, so we wanted to check what security is actually in place. We considered several approaches to this. One approach could be to look at one platform alone, e.g. Xbox Live or PlayStation Network. But since we could not find any previous work conducted in this area of research we decided that we should look at as many platforms and consoles as possible. And since this thesis concerns itself with fairly new hardware we had to make a choice as to which consoles we were to test. Unfortunately we did not have the possibility of testing the PlayStation 3. There were several reasons for this; The PS3 was released March 23, 2007 in Norway, thus giving us a rather short timeline for testing purposes. It is also a rather expensive console, and it would be difficult to get hold of one early after the release.

Another possible approach to this subject is to take a historical look at game consoles. How game consoles have evolved from being one game machines attached to a TV into the media centres of today. During this period there has been several security related incidents, and the more complex the consoles get the higher possibility of something going wrong.

One thing we considered was to take a closer look at the legal environment around games and game consoles. The End User Licence Agreements is something that most users just agree to, without really considering what they are agreeing to. We considered taking a closer look at the EULAs of the different game consoles and for some games. But we came to the conclusion that this should probably be done by someone with more experience with legal terms and laws in general.

Yet another angle we considered was to take a closer look at the users and usage of game console. It is the users that often will feel the greatest impact if security related issues arise. There is also the question of protection of personal information in game and virtual worlds. We decided that we wanted to take a closer look at this. The most vulnerable users of games and game consoles are children, especially young children.

They consider playing games to be fun and a game console to be a toy. But with the advent of online gaming this changed. Playing a game online can be much more than just a toy and children should be made aware of this.

We therefore decided to conduct a survey, to balance our findings from the technical experiments. When looking at both the technical security solutions and information from a survey into how parents consider their children's safety when playing games online, we can hopefully get a bigger picture of how secure it is to use a game console.

3.3 The technical experiments

The technical experiments bases themselves on the equipment and software described in chapter 4. Instead of doing very detailed technical experiments on one platform we decided to do a broader survey of game consoles, and not go so much in detail on each platform. This was chosen because we were not able to find any previous work in this area that had conducted similar experiments.

The experiments themselves were conducted in several phases. Firstly the game consoles in question were, as far as possible, connected to a network without any Internet connection and then subjected to the tests. This was done in order to examine the consoles before they interacted with their respective services online. Most game consoles when connected to the Internet are forced to download updates of the operating software, and these updates could contain security related fixes. In order to avoid these possible updates, the experiments were first run in an environment without a connection to the Internet.

When the testing in this environment was finished, the consoles were connected to the Internet for the first time. In most cases this resulted in a forced update of the operating software. When this was done the consoles were again subjected to the same tests as before, to determine whether or not their behaviour had changed.

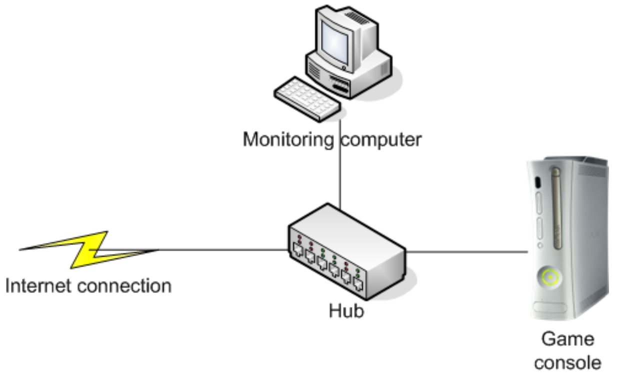

Figure 1: The setup of the test network.

We also did some monitoring in order to find out how the consoles interacted with their online services. This was done by using a program called Wireshark (described in chapter 4). But since most modern network equipment is designed to only send network traffic to and from its respective targets, and not broadcast it to other equipment on the network, it can be rather difficult to be able to monitor the traffic between the game console and the Internet. This was solved by using a hub, see figure 1. This type of network device takes all traffic from one source interface, and sends it out on all the other interfaces. The hub was always placed somewhere in between the game console and the Internet uplink connection. A computer connected to this hub can then see all traffic sent between the game console and the Internet.

All these tests were done in order to give us a quantity of data that could be used to say something about the security of the give console and its respective service on the Internet. The interpretation of the collected data will be a qualitative assessment of the quantitative data.

3.4 The questionnaire

The questionnaire (for the Norwegian questionnaire see 9.1 and for the English translation see 9.2) was conducted in order to be a counterpoint to the technical experiments. We decided that the target of the questionnaire should be parents with children in grade school. We wanted to assess how parents interact with children and their use of game consoles and games played on the Internet, whether or not the children had had any schooling in how to use the Internet in a safe way and how parents thought children used their personal information on the Internet and in virtual worlds.

The questionnaire was developed over several weeks, and went through many iterations. When we felt that we were nearing a finished version we contacted the local government and asked them if we could conduct the survey in local schools with their authorisation. Unfortunately, when we finally got permission to do the survey, we were severely behind schedule. The questionnaires were sent out on Wednesday 16 of May, and were collected on Friday 25 of May. This was a somewhat shorter time span than originally planned. We did get some answers the week after this, but not many. We sent out 1146 questionnaires to 5 local schools in the area around Gjøvik city. The schools were demographically chosen so that we covered big and small schools, both in the city and out on the countryside. Out of the 1146 questionnaires we sent out, we got back 322 filled out surveys that we could use. This gives us roughly a return rate of 28 %.

4 Equipment

4.1 Chapter summary

This chapter takes a look at some of the hardware and software we have used in this project. Each game console has its own subchapter, with information about the hardware used in each console. There is also a description of most of the software that was used during the project.

4.2 The consoles

A lot of the information about the hardware in game consoles is often speculations, since the companies selling them don't want to give the developers of modification chips any kind of help in their work. This usually means that the information found about the newest consoles might be educated guesses, while the information about older consoles often has been confirmed.

4.2.1 PlayStation 2

The PlayStation 2 is part of the sixth generation of game consoles. It was the sequel to the immensely popular PlayStation. It was released in March 2000 in Japan and subsequently in October and November in North America and Europe. The console has sold over 110 million units worldwide [44], making it the most popular game console in history, and has gone trough several revisions in its lifetime. It is also by far the game console that has had the longest life span. Released in 2000, it still sells quite well world wide, often contributed to the enormous game library available. The specifications of the PlayStation 2 are [45, 46, 47]:

- 300 Mhz 128-bit "Emotion Engine" CPU.
- 32 MiB Direct Rambus or RDRAM.
- "Graphics Synthesizer" GPU clocked at 150 MHz.
- CD/DVD drive.
- 10/100 Mbps RJ-45 Ethernet network port in some models.
- Weight: Varies with the revision.
- Dimensions: Varies with the revision.

When compared with its main rival at the time, the Xbox, the PlayStation 2 might seem somewhat underpowered. Most of the revisions did not have built in support for Ethernet networking, and did not have a hard drive. However, it came with an expansion bay, making it possible to add network or hard drive support. It should also be noted that the PlayStation 2 was specifically designed to be a game console, while the Xbox used many generic computer parts in its design. The result of this is that the gap in performance between the PlayStation 2 and the Xbox is not as large as might be expected.

The PlayStation 2 has been released in as many as 14 versions, and we used a version 3 PlayStation 2 during this project.

4.2.2 PlayStation 3

The PlayStation 3 is Sony's contribution to the seventh generation of game consoles. It was released in November 2006 in Japan and the US and in March 2007 in Europe. In between it was released several other places in the world. Because of these release dates we did not have time to include the PlayStation 3 in our research, but since it will be referenced several times we include some information about it none the less. The console was originally released in two versions, basic and premium. The basic configuration has a built-in 20 GiB hard drive, while the premium has a 60 GiB hard drive. The specifications of the PlayStation 3 are [48, 49, 50]:

- 3.2 GHz Cell processor.
- 256 MiB XDR DRAM.
- nVidia G70 based graphics processor RSX 'Reality Synthesizer' with 256 MiB GDDR3 VRAM.
- Support for Blu-ray Discs, CDs and DVDs.
- An 20 or 60 GiB hard drive depending on version.
- Gigabit Ethernet network port.
- Weight: 5 kg.
- Dimensions: 325 x 98 x 274 mm.

4.2.3 PlayStation Portable

The PlayStation Portable, abbreviated PSP, is Sony's handheld gaming platform for the seventh generation of game consoles. It was released in December 2004 in Japan, North America in March 2005 and in Europe and Australia in September 2005. The PlayStation Portable was designed to play games, listen to music and watch movies. All media is run from the optical drive that uses the Universal Media Disc format. The specifications of the PSP are [51, 52]:

- 110 mm, 16:9 widescreen TFT LCD screen with resolution 480 x 272 pixel and 16.77 million colours.
- PSP CPU (System clock frequency 1 - 333MHz).
- 32 MiB main RAM and 4 MiB embedded DRAM.
- Graphics chip clocked at 166 MHz with 2 MiB embedded memory.
- Universal Media Disc optical drive
- Memory Stick Duo slot
- Built-in 802.11b WLAN capabilities.
- Weight: approximately 280g (including battery).

- Dimensions: 170 x 74 x 23 mm.

The built-in WLAN capabilities can be used to create an ad-hoc local network for multiplayer gaming supporting up to 16 PSP's in one such network. One has to act as a host for the game, and the others connect to this one. It is also possible to connect the PSP to the Internet through a WLAN capable router with an Internet connection. This can be used to play games online, browse the Internet via the Access Co. NetFront browser or download files to the Memory Stick. In our testing we used two PSP's, both with version 2.71 of the firmware originally installed. They were later upgraded to the latest firmware available at the time, version 3.40.

4.2.4 Xbox

The Xbox is part of the sixth generation of game consoles, and was Microsoft's first attempt to get into the video game marked. It was released late in 2001 in North America, and early 2002 in the rest of the world. According to [10, 53, 54, 55] the specifications of the Xbox is:

- 733 Mhz Intel Celeron-class processor.
- 64 MiB DDR SDRAM.
- An nVidia GeForce 3 based Graphics Processing Unit running at 233 MHz.
- An nVidia Media Communications Processor.
- DVD drive.
- An 8 or 10 GiB hard drive formatted with the FATX file system.
- 10/100 Mbps RJ-45 Ethernet network port.
- Weight: 3.86 kg.
- Dimensions: 320 x 100 x 260 mm.

When compared to its main competition, the PlayStation 2, the Xbox seems to be fairly more advanced having both a built in hard drive and Ethernet network port. But it is also very similar to a generic computer anno 2001-2002. Some of the hardware was specifically designed for the Xbox, but much of it comes directly from the computer world. In this way Microsoft saved both money and time in development.

The modified Xbox used in the testing is a version 1.6 and has been fitted with an Aladdin XT modchip. It runs the Evolution-X dashboard version 3935.

4.2.5 Xbox 360

The Xbox 360 was the first of the seventh generation of game consoles to be released. It was released late 2005 in the US, Canada, Europe and Japan. Originally the Xbox 360 came in two models, the Core System and the Premium System. The Premium System had a built-in hard drive of 20 GiB, wireless controller, a lot of extra cables for connecting to network and TV and a month free Xbox Live gold membership. In 2007 Microsoft announced the Xbox 360 Elite, the third and most expensive of the Xbox 360 to date. It will have a built-in 120 GiB hard drive, and support for High-Definition Multimedia

Interface (HDMI). According to [56, 57, 58] these are the specifications of the Xbox 360:

- Custom PowerPC "Xenon" with 3 cores all clocked at 3.2 GHz.
- 512 MiB of 700 MHz GDDR3 RAM.
- Custom ATI Graphics Processor "Xenos" with 10 MiB built-in RAM.
- 12X DVD drive with option for purchasing external HD DVD drive.
- An 20 or 120 GiB hard drive depending on model.
- 10/100 Mbps RJ-45 Ethernet network port, with option for purchasing added WLAN network support.
- Weight: 3.5 kg.
- Dimensions: 83 x 309 x 258 mm.

The seventh generation of game consoles shows a huge leap in hardware performance. The Xbox 360, and its main competitor the PlayStation 3, both run on multiple-core CPUs, both has support for High-Definition images and they both have built-in hard drives. Upon release of the Xbox 360 Microsoft update its Xbox Live service in order to accommodate the new console.

4.2.6 Nintendo Wii

The Nintendo Wii, formerly known as Nintendo Revolution, is Nintendo's contribution to the seventh generation of game consoles. The Wii was launched late in 2006. Nintendo has taken a very different approach to their game console this time around, compared to Microsoft's Xbox 360 and Sony's PlayStation 3. Where they have developed consoles with a lot of focus on high-end hardware, Nintendo is trying to change the way we play on game consoles. This has resulted in on of the smallest game consoles to date, with some major changes in the way we operate the game console. The Wii uses a remote like point-and-click device in order to operate, and this remote is motion sensitive. The motions performed with it are transferred to the console trough the use of Bluetooth, and infrared light to perform pointing on the screen. The specifications of Wii are, according to [59, 60, 61], this:

- 729 MHz IBM PowerPC based "Broadway" CPU.
- 24 MiB "internal" 1T-SRAM integrated into graphics solution, 64 MiB "external" GDDR3 SDRAM.
- 243 MHz ATI "Hollywood" GPU.
- Disc drive compatible with 8cm GameCube discs and 12cm Wii discs.
- 512 MiB built-in NAND flash memory.
- Built-in 802.11b/g WLAN capability, compatibility with USB 2.0 to Ethernet.
- Weight: 1.2 kg.
- Dimensions: 44 x 157 x 215.4 mm.

The Wii has a feature called WiiConnect24. When this feature is on, the console will automatically update some of its features, such as the Forecast Channel or the News Channel. But there is also an additional functionality that can be enabled, and that is the possibility of a Standby Connection. This option makes it possible for the Wii to send and receive information on the Internet when it is in standby mode. It also makes it possible to download firmware updates. When this option is off, the Wii only interacts with the Internet when we actively use it [62].

4.2.7 Nintendo DS

Nintendo DS is Nintendo's latest handheld game platform in a long line of such devices. Originally released in 2004, a later revision of the system called the Nintendo DS Lite was released in 2006. The Nintendo DS notably separates itself from the PlayStation Portable with the fact that is has two screens, one of which is touch sensitive, and that it has a clamshell design. The specifications of the Nintendo DS Lite are [63, 64]:

- Two 77 mm TFT LCD screens with resolution of 256 x 192 pixels. The lower screen is touch sensitive.
- CPUs: One ARM9 and one ARM7, each responsible for different tasks.
- Built-in 802.11b/g WLAN capabilities.
- 1 Nintendo DS cartridge slot, 1 Nintendo Game Boy Advance cartridge slot
- Weight: 275 g.
- Dimensions (closed): 133 x 73.9 x 21.5 mm.

As with the PSP the Nintendo DS has the possibility to connect to the Internet through a WLAN connection. This can be done either with a WLAN capable router or through a Wi-Fi USB connector connected to a computer.

4.3 The software

The software we used during this project was chosen for several reasons. Firstly we don't get that much more information from commercial software, since this software often is aimed against commercial platforms. They usually also cost a lot of money. And since we only use software that is free of charge and openly available, it is easier for others to replicate the results.

4.3.1 Nmap

Nmap [65], short for Network Mapper, is an open source, free utility used to audit the security and explore networks. It is easy to use, with a command line interface that works on many different operating systems. It is also possible to use it with a GUI frontend, often provided by third parties.

It has a lot of different methods of scanning machines on a network. It has methods of host discovery, different scan techniques, service and operating system detection, firewall and intrusion detection system evasion and packet spoofing.

4.3.2 Nessus

Nessus [66] is another free network vulnerability scanner. Where Nmap is targeted more against detecting computers and services on a network, Nessus is used to detect specific vulnerabilities on a given machine. Nessus comes with its own port scanner, but it can also be used in conjunction with Nmap if desired. It contains a large database of known vulnerabilities, and has several thousand plugins to perform different tasks.

Nessus is one the most used vulnerability scanners available today. It has its own scripting language, Nessus Attack Scripting Language (NASL), which makes it possible to write custom exploits to perform on your network. Nessus also has a "safe check" option, and when this option is turned off Nessus's vulnerability tests might try to make unstable or unsafe services crash.

4.3.3 Wireshark

Wireshark [33] is a free open source network packet sniffer, formerly known as Ethereal. It is used for network traffic analysis, network troubleshooting, software development where networking is involved, protocol development and is often used by educational institutions. The program listens to all incoming and outgoing traffic on a network interface, and when the listening is done, lists the individual packets that were "sniffed" on the network.

By using software like Wireshark it is possible to se in minute details what is happening on you network interface, and use this information to e.g. debug software, but it is also possible to glean potential sensitive information, e.g. passwords for mail services. It can also be used to learn how different software and hardware behave on a network.

One of the major advantages of Wireshark as opposed to similar software is the well developed tools for capture and view filtering, making it a lot easier to filter out the traffic that we are specifically looking for.

4.3.4 Metasploit Framework

The Metasploit Framework [67] is a tool which lets its user choose or configure an exploit to use against a given system. When an exploit is found on a system, and configured in the Metasploit Framework, it is possible to add a payload. This separation of exploit and payload makes it easy to use the same payload on several different exploits, without having to create it again.

This tool is often used to test the security of computer systems, perform penetration testing and Intrusion Detection System testing.

4.3.5 SPSS

SPSS (Statistical Package for the Social Sciences) [68] is a program used to conduct statistical analysis. We have used this program to conduct analysis of the statistical data we collected in our survey.

5 Technical results

5.1 Chapter summary

This chapter contains the results from our technical experiments. Each console and the results for that console are presented. There is also some information about the results we found when looking into the service platforms of some of the game console manufacturers. There is a varying degree of details and information, depending on how much we were able to find.

5.2 The modified Xbox with the modchip enabled

Open ports:

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
731/tcp	open	netviewdm3
731/tcp	open	xboxdebug Microsoft Xbox Debugging Kit

Table 1: Open ports on modified Xbox with modchip enabled

Open protocols:

Protocol	State	Service
1	open	icmp
6	open	tcp

Table 2: Open protocols on modified Xbox with modchip enabled

This is a summary of what we found on the modified Xbox. As described in 4.2.4, the Xbox runs an Evolution-X dashboard replacement. This dashboard comes with built-in support for running FTP and Telnet server, which explains respectively the open ports 21 and 23. The port 731 is reported as being part of IBM's Netview system, a monitoring program based on the Simple Network Management Protocol.

The problem with this specific port, and the service running it, is that it is highly unstable when it comes to network probing. When running the discovery and port scans, it causes no problems. But when running the operating system and version detection scans we get some trouble. In most cases the modified Xbox just freezes during these scans. We traced this port number back to a service called RD Tools, which is a service for remote development. When this service is turned off, the Xbox does not freeze during scanning. But at other times it would not freeze during the same scan, even though the service was turned on. Why this is so, we were not able to ascertain. But the few times it didn't freeze, different results were found. The service information now reported was "xboxdebug Microsoft Xbox Debugging Kit".

When it comes to the results from the Nmap port scan, these also varied somewhat. Most of the port scans that Nmap runs came up with the same results. But Nmap also has a scan type called "TCP Connect()", explained by the manual as

> asking the underlying operating system to establish a connection with the target machine and port by issuing the connect() system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt.

This scan type takes a very long time to complete, using several hours to completely scan the whole range of ports. It also produces varying results. The ports this specific scan detected, was not always detected at a later time with the same scan. And at subsequent scans some ports are not detected, and others are. The resulting state "filtered" means that "Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port".

The tools we used were also able to determine what protocols the target support, in this case it was ICMP and TCP. One consistent thing we discovered is that the tools we used are not sure what they are dealing with. They often give varying results depending on when the scan is performed, and they also have problems detecting what kind of device it is. When the modchip is enabled, we are most of the time able to detect that it is a game console being scanned.

On the other hand, we also came across some inconsistencies. It varies a lot how the Xbox behaves after it freezes. When this happens we sometimes get positive results that the Xbox is running Microsoft Windows 2003/.NET. But we also experienced that after the Xbox freezes, no open ports, no vulnerabilities and no services are detected.

5.2.1 Known buffer-overflow vulnerabilities

On thing we did discover is that the Evolution-X dashboard has known buffer-overflow vulnerabilities [69]. They were first reported late 2004, and by the time of writing in spring 2007 there has yet to be released a fix.

5.3 The modified Xbox with the modchip disabled

When turning the modchip off, the Xbox is supposed to behave as an unmodified Xbox does. The first tests that we ran were with the Xbox on a closed network with no Internet connectivity, and no connection to the Xbox Live service. When scanned in this condition we were not able to find any information about the Xbox, other than that it was on and responded to network traffic. When connecting the Xbox to a network with Internet connectivity, the results came out the same. We found no other information than that the Xbox was up and running, and responding to network traffic.

5.4 The Xbox 360

Open ports:

Port	State	Service
1026/tcp	open	LSA-or-nterm
1027/tcp	open	upnp - XBox 360 XML httpd (Serial number ************)

Table 3: Open ports on Xbox 360

This is a summary of what we found on the Xbox 360. There is one service running on port 1026 or 1027, it varies. It is a Universal Plug and Play (UPNP) service used for finding other UPNP devices on a network, and quickly and easily set up a connection between them. It varies what port the service responds to, and also what information we can gather from it. At some instances it will give us nothing, at other times it gives us the serial number of the Xbox 360. But by connecting to the service through a web-browser we get quite a lot of information. We find out that it is in fact an Xbox 360, we get the serial number, the Universally Unique Identifier (UUID) for the Xbox, and some information about the UPNP service.

When scanning the Xbox 360 we get somewhat differing results. It was reported that the Xbox 360 is running a web server on port 1026/1027 and we are usually presented with one or more possible ways to attack the Xbox 360. We have not been able to confirm that any of these attacks works. It seems that yet again the tools used are not sure what they are dealing with.

When looking at the network based security of the Xbox and the Xbox 360, it is impossible to ignore the connection between the consoles in question and the Xbox Live service.

5.5 The Xbox Live service

Since we are looking for network based attack vectors we decided early on that we should take a closer look at the Xbox Live service, and how it interacts with the Xbox. Xbox Live is a service provided by Microsoft to support online multiplayer gaming and to deliver content to the Xbox. It was launched in 2002, and was updated on the release of the Xbox 360 to accommodate the new console. The service comes in two flavour, silver and gold membership. The silver membership is free and provides gamers with the opportunity to maintain a gamer profile, use the friends list, access the Xbox Live Marketplace where we can download trailers, game demos, arcade games and more. The gold membership is one that users have to pay a monthly fee in order to get access to. By upgrading to gold we get access to all that the silver membership has access to, but on top of this we get access to online multiplayer gaming, Gamerscore that keeps track of your gaming achievements and much more [70].

When signing up for use of the Xbox Live service, Microsoft requires that users have access to an account that is part of their Windows Live ID service (formerly known as .NET Passport). This is a single sign-on system that makes it possible to sign on to many services using one account. When the sign-up process is over and we log onto Xbox Live for the first time we are forced to download and install the newest firmware update. When all this is finished we can begin using the Xbox Live service.

The ports that needs to be open in any firewalls to be able to use the Xbox Live service, and their use as reported by the Internet Assigned Numbers Authority [71], can be seen in table 4:

Port	Service
53/tcp	Domain Name Server
53/udp	Domain Name Server
88/udp	Kerberos
3074/tcp	Xbox game port
3074/udp	Xbox game port

Table 4: Xbox Live ports

5.5.1 Kerberos

Using Wireshark we analysed the network traffic going between the Xbox and the Live servers. The Live service relies on the Kerberos protocol for authentication. A normal run of the Kerberos protocol can be seen in figure 2, together with a brief explanation of how it works.

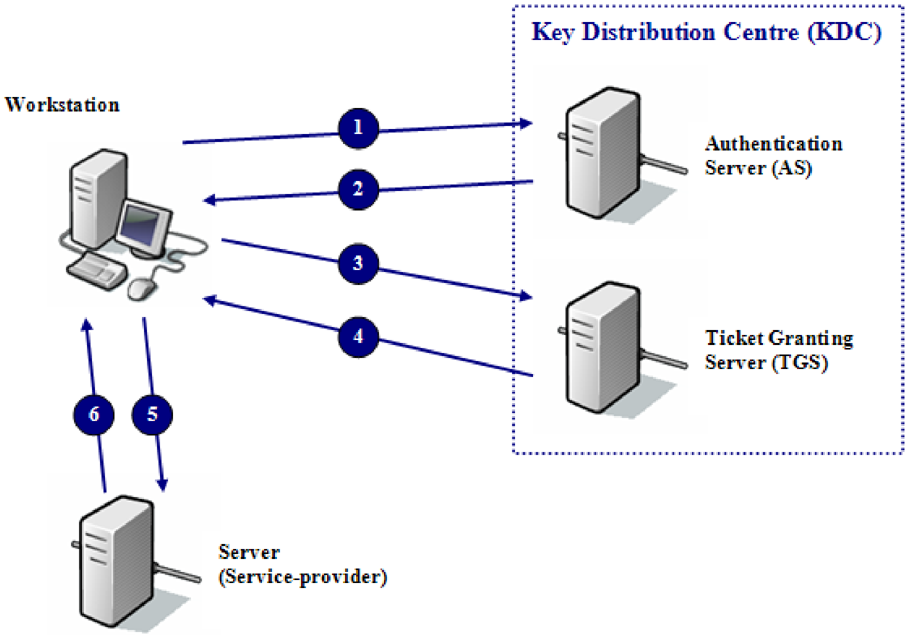
Key Distribution Centre (KDC)
Workstation
1
2
3
4
5
6
Authentication Server (AS)
Ticket Granting Server (TGS)
Server (Service-provider)

Figure 2: An overview of a normal Kerberos protocol run.

1. The first step is to request a Ticket Granting Ticket (TGT) from the Authentication Server (AS).
2. If the client is authenticated at the AS, the AS sends back a TGT together with a session key that is used to communicate with the Ticket Granting Server.
3. Upon receiving the TGT the client now turns to the TGS to get a Service Granting Ticket (SGT).
4. If the session key from step 2 checks out, the TGS sends a SGT together with another session key that is used to communicate with the Service Provider.
5. The client now sends a request for use of a service, together with the SGT and the session key from step 4.
6. If everything checks out, the client is granted access to the service.

This is how a normal Kerberos protocol run takes place. But since Microsoft controls the Authentication Server, the Ticket Granting Server and the service itself, not all steps of the protocol is always needed. When monitoring the process with Wireshark, we discovered that it depends on what service we request.

The Kerberos protocol always runs twice, or simultaneously. This is done in order to authenticate both the user and the Xbox itself. When logging onto Live from the dashboard, only the first four steps of the protocol run is performed. The last two steps is omitted. When logging onto Live from inside a game, in our testing we used Halo 2, the full protocol run is executed. The protocol is run every time we request the use of a new service, e.g. Friends, Matchmaking, Statistics. Figure 3, from [72], gives an outline of how the system works. It is the Security Gateway that authenticates and decrypts all Xbox Live traffic. The tickets that are granted typically have a lifespan of 24 hours.

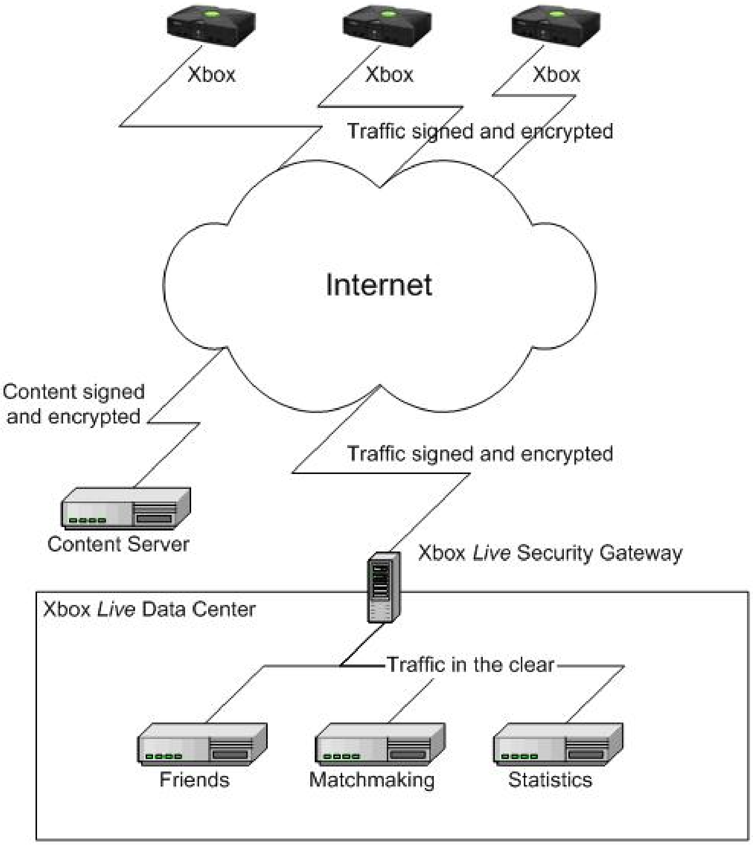
Xbox
Xbox
Xbox
Traffic signed and encrypted
Internet
Content signed and encrypted
Traffic signed and encrypted
Content Server
Xbox *Live* Security Gateway
Xbox *Live* Data Center
Traffic in the clear
Friends
Matchmaking
Statistics

Figure 3: An overview of how the Xbox Live system works

5.5.2 Other security protocols

After the tickets have been obtained all subsequent traffic is encrypted and authenticated. For authentication of network traffic HMAC-SHA-1 [73] is used. At the same time console-to-console and console-to-game server traffic is encrypted with DES, while important console-to-Live traffic (billing, sign-up, sign-in) is encrypted with 3DES [72, 74]. To create session keys to be used in the authentication and encryption of the traffic, the Xbox uses the Diffie-Hellman key exchange protocol. But it is important to remember that these are things that Microsoft probably can change at any given time.

5.5.3 Protocol modifications

The Xbox uses modified version of TCP and UDP, together with Xbox Voice and Data Protocol (VDP), in order to communicate with the Internet. All of these traffic types are then tunnelled over UDP. This is done for one reason; when all traffic travels over UDP the question about Network Address Translation (NAT) device compatibility can mostly be ignored. A NAT device makes it possible for several computers to share one single IP-address, but they often also works as a firewall. But by using only UDP this problem can be ignored, since NAT devices usually relays all UDP traffic by default.

All traffic to and from the Xbox is tunnelled over UDP in this manner, even UDP. The only exception we found is when downloading firmware updates. These are downloaded using normal TCP.

5.6 PlayStation 2

The PlayStation 2 is a console from the sixth generation of game consoles, and most versions of the console were not delivered with a network card. On a later stage a network card that could be fitted to the expansion bay at the back of the PlayStation was released [75].

When the network card is not in use, it is completely shut of. Whether this is a security feature, a power saving scheme or something else is not known, but it works in the favour of network security none the less. It means that as long as the network card is not in use, there is no possible way to connect to the console over the network.

We were not able to find any default open ports on the PlayStation, it all depends on what services that we are connected to on the Internet. But the use of online possibilities never really took off when it came to the PS2.

5.7 PlayStation Portable

The PlayStation portable, with it's built in WLAN, is fairly easy to connect to the Internet through a WLAN capable router. When first connected to the Internet we are not forced to update the firmware, but the PSP has a function for doing this upgrade. We first tested with the original firmware, and then later upgraded it to see if the PSP behaved differently after the upgrade.

Open protocols:

Protocol	State	Service
1	open	icmp
2	open|filtered	igmp
6	open	tcp
17	filtered	udp

Table 5: Open protocols on PlayStation Portable

We found no default open ports on the PSP, but the network protocols available is listed in table 5. This is the same on both PSP's, and with both versions of the firmware. In the case of all the other game consoles we have tested the tools we used have not been able to determine the operating system. But with the PSP the operating system is reported to be "OpenBSD 4.0 (x86)". Whether or not this is correct is difficult to ascertain, but it might be the case that Sony has used the network stack from the OpenBSD operating system on the PSP.

We found some minor issues with the PSP. First of all it is reported that it is possible to determine the exact time on the remote host, through the use of ICMP timestamp requests. Secondly it is reported that the PSP accepts IP packets with loose source routing. This feature can be used to circumvent poorly designed IP filtering. These are reported consistently all the time. But as we have seen before, also with the PSP we get several results that are inconsistent.

5.8 Nintendo Wii

Open ports:

Port	State	Service
68/udp	open|filtered	dhcpc

Table 6: Open ports on Nintendo Wii

Open protocols:

Protocol	State	Service
1	open	icmp
6	open	tcp
17	filtered	udp

Table 7: Open protocols on Nintendo Wii

This is a summary of what we found on the Wii. The only port that was found, was found with the Connect() scan method, described in 5.2. The resulting state open|filtered is a state in which an open port does not respond to probing. The port 68 and the underlying service dhcpc is part of the DHCP system that Wii uses to automatically get assigned an IP-address from a DHCP server. As part of this DHCP system Wii only asks for an IP-address when it is needed, not on boot up. When starting a service that requires access to the Internet, Wii asks for an address from the DHCP server, and when it is finished with the Internet access it releases its IP. This can make it somewhat difficult to scan the Wii, since there is no guarantee that it will keep its IP for the duration of the scan. This also helps defend against network based attacks, since the Wii will not at all times actually have an IP-address.

5.8.1 Vulnerability in the Wii

When scanning the Wii with Nessus we found a known vulnerability [76]. This is a confirmed vulnerability in Wyse Winterm thin clients running a specific firmware version. It has also been confirmed on three different Wii's. When sending IP packets with a zero in the IP-options length field to the Wii, it crashes. When the packet has been sent, next time we try to use the Wii it hangs, either the image just freezes or it goes to a black screen and then freezes. It stops responding to the Wii Remote; even the power off button on the Remote does not work. We have to turn the console completely off, before it will respond to any input again. The Wii is also effected by this vulnerability when in standby mode with WiiConnect24 turned on, see 4.2.6 for a description of WiiConnect24.

We did some testing exploiting this vulnerability during some critical operations. When using the Wii Shop to buy games, we have to have Wii Points. Each game is worth a certain amount of these points, and they can be bought in the Wii Shop. This is done using a credit card. We tried running the exploit in the middle of a credit card purchase, and the Wii went into a loop. Since it no longer could send or receive traffic, the operation never finished and we had to take the power. But the transfer got through none the less. We also tried disrupting the actual download of a game, but this has a feature where you can redownload a game that was aborted.

5.8.2 Wii network services

The Wii offers a range of services to its users. With the latest firmware update at the time of writing there are five services on the Wii that requires Internet access to work. These are Wii Shop, Forecast Channel, News Channel, Internet Channel and Everybody Votes Channel. The Forecast Channel and the News Channel sends or receives no personal information, and therefore there is no need for much security. The Internet Channel is basically an Internet browser developed by Opera for the Wii [77]. Everybody Votes is a channel where Nintendo asks its users questions like "Do you play an instrument?" or "What came first, the chicken or the egg". The users then give their answer, and are given the opportunity to guess what the majority of the users will answer. Since this information can be seen as personal its transfer over the Internet is also encrypted with TLS [78].

The Wii Shop is the service with the most uses, and also with the most potential personal information being transmitted. In the Wii Shop we can buy old games from game systems such as Nintendo Entertainment System, Super Nintendo Entertainment System, Nintendo 64, Sega Mega Drive/Genesis systems and more. Theses are playable in the Wii's virtual console system. It is also possible to download software updates to the Wii through the Wii Shop. This means that there is a lot of information being transferred that needs to be protected, including payment information such as credit card information. Therefore most of the information exchanged with the Wii Shop is encrypted with TLS. All of the other services that send personal information over the Internet is also encrypted.

Table 8 shows the ports that needs to be open in any firewalls to be able to use the Wii network service [79], and their use as reported by the Internet Assigned Numbers Authority [71]:

Port	Service
80/tcp	World Wide Web HTTP
443/tcp	http protocol over TLS/SSL
28910/tcp	unassigned
29900/tcp	unassigned
29901/tcp	unassigned
29920/tcp	unassigned

Table 8: Wii network service ports

The first time we connect the Wii to the Internet we are forced to update it with the latest firmware, just as is the case with the Xbox Live system. These firmware updates are not encrypted. Neither is updates downloaded from Wii shop, such as the Internet Channel update.

5.8.3 Akamai Technologies

Nintendo is using the Akamai Technologies content distribution system to deliver content too the Wii [80]. Akamai provides a distributed global platform for Internet content cashing and distribution. This means that when requesting services on the Wii, there is not a centralised server responding to requests from all over the world, but a lot of servers all over the world responding to Wii's in their area.

5.8.4 WiiConnect24

When WiiConnect24 is enabled with the standby option on, the Wii sends and receives information on the Internet all the time. At regular intervals the Forecast Channel and News Channel receives its updates, but it is also possible for the WiiConnect24 to receive firmware updates and other information while the console is in standby mode.

5.9 Nintendo DS

Open protocols:

Protocol	State	Service
1	open	icmp

Table 9: Open protocols on Nintendo DS

This is a summary of what we found on the Nintendo DS. There are by default no open ports, and we only found one open protocol.

The DS behaves very much like the Wii in some aspects. It has the same feature where it releases its IP-address when not needed, which makes it rather difficult to attack it since it seldom has an IP for a long time. With its built-in WLAN support it is easy to connect the DS to the Internet, but it has no functionality for updating the firmware. It also does not have a built-in function to handle connectivity with a WLAN capable router. This is something that is done in each game that needs this functionality.

The Nintendo DS has, as the PSP, the possibility to create ad-hoc gaming zones. Several games support a structure where you only need one copy of the game. The DS with the game copies some content over to all the others, and so they can play together.

It also comes with a built-in function called PictoChat. This is a chat function, making it possible to locally create channels in which users can chat with each other. The range of this local ad-hoc functionality is somewhat limited. According to Nintendo, the range of the WLAN in the DS is approximately 9-30 meters (30-100 feet) [63]. This fits with our own informal measurements.

As was the case with the PlayStation Portable, the Nintendo DS is also susceptible to accept IP packets with loose source routing.

6 Results from the questionnaire

6.1 Chapter summary

These are some of the results from the questionnaire. We have chosen not to present all the results, since much of the data collected can not be used to answer our research questions. Some of the data will be used to create background information and different indexes, in order to compare these against individual topics. The statistical data not used by this thesis might be used by other future projects.

Firstly we present a basic frequency count of some of the questions that interest us. Secondly we create several indexes and see how the different questions behave when compared against the indexes.

6.2 Question 23

I feel that playing computer/video games on the Internet is unsocial

It is a common perception today that playing games online is an unsocial act. This perception has survived for a long time, and is till to this day common. It is not the task of this project to question the truth of this statement, but we wanted to see if this perception still exists. Therefore we asked the question: "I feel that playing computer/video games on the Internet is unsocial". The results can be seen in figure 4.

If we add together those who agree and those who agree some, a little over 46 % of the people asked feel to some degree that online gaming is unsocial. But at the same time 33 % say they neither agree nor disagree to the statement. 19 % disagree or disagree some.

As we see, there are still many people who believe that playing games on the Internet is unsocial. We believe that this perception is something that will change over time. It has become increasingly more popular with social games over the years. Concepts like SingStar, Guitar Hero and MMORPG (Massive Multiplayer Online Role-Playing Games) creates a very different game experience than has been seen before. As more and more of these types of games are launched, the perception that online gaming is unsocial might change.

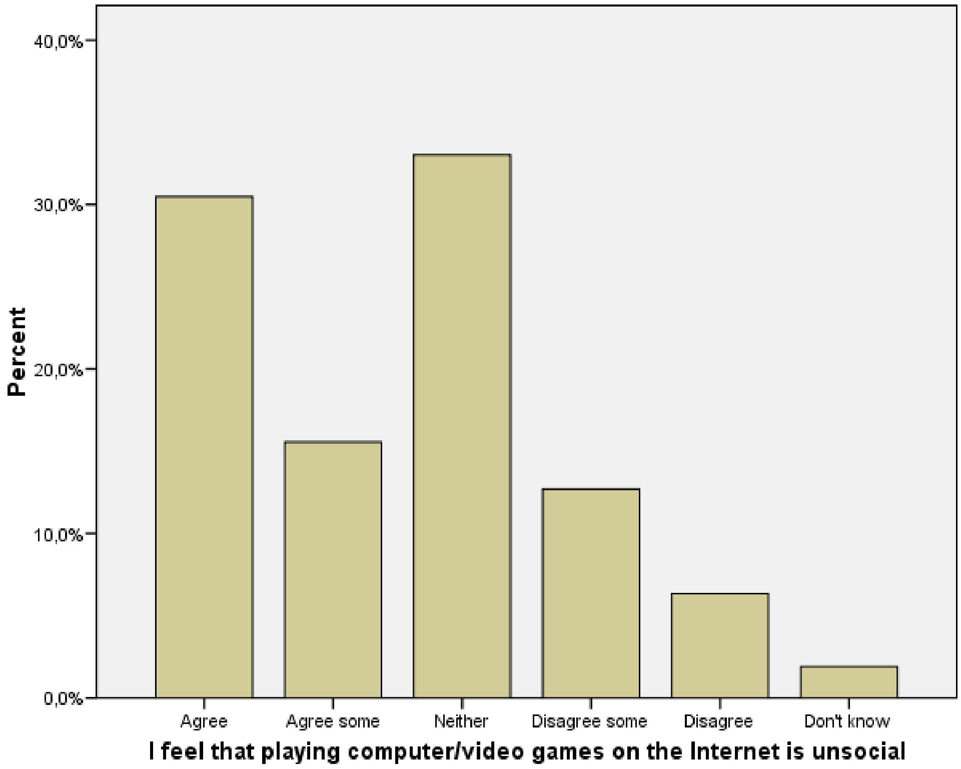

Figure 4: Question 23: I feel that playing computer/video games on the Internet is unsocial

6.3 Question 24

I feel that it is smart to limit children's time usage when it comes to playing computer and video games

It is also quite common to limit children's use of games, in order to make sure they don't spend too much time on it. We wanted to find out how common this is. The results to this question can be seen in figure 5.

Again, it is not within the scope of this paper to discuss whether or not this is the right thing to do. But we can see that if we add together those who agree and those who agree some, we get that over 94 % of the people who answered thinks that it is smart to limit their children's time spent on computer and video games.

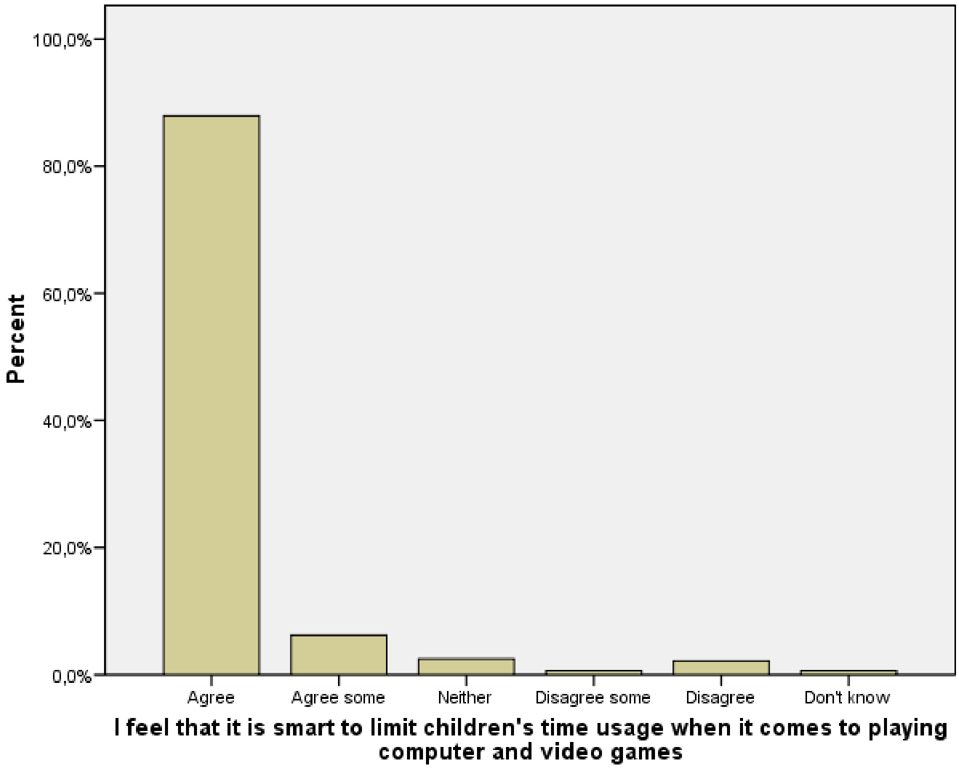

Figure 5: Question 24: I feel that it is smart to limit children's time usage when it comes to playing computer and video games

6.4 Question 25

I think children can become violent by playing computer/video games that contains violence

One topic that always comes up when we talk about games and online gaming is violence. For many years there have been those who claim that violent video games can make children behave violently. There has been conducted countless studies on this topic, together with the topic of violence in other entertainment media. Again it is not the topic of this thesis to answer this question, but we were interested to see what parents feel about the topic. The results is depicted in figure 6.

As we see, those who agree or agree some make up for a little over 53 %. Those who disagree to some degree constitute a little over 15 %. With this particular question it is possible to argue that the category "neither" probably can be interpreted as "don' know", which gives us a total of 31 % who are not sure if children can become violent by playing violent computer and video games.

As mentioned it is not the purpose of this paper to argue this question, but we will cite some of the arguments used in the debate. Some argue that violent video games make children more violent in their behaviour outside the game. This, it is argued, can be seen by looking at the amount of senseless violence in today's society. Especially episodes like the Columbine school shooting and the Virginia Tech shooting is stressed as episodes

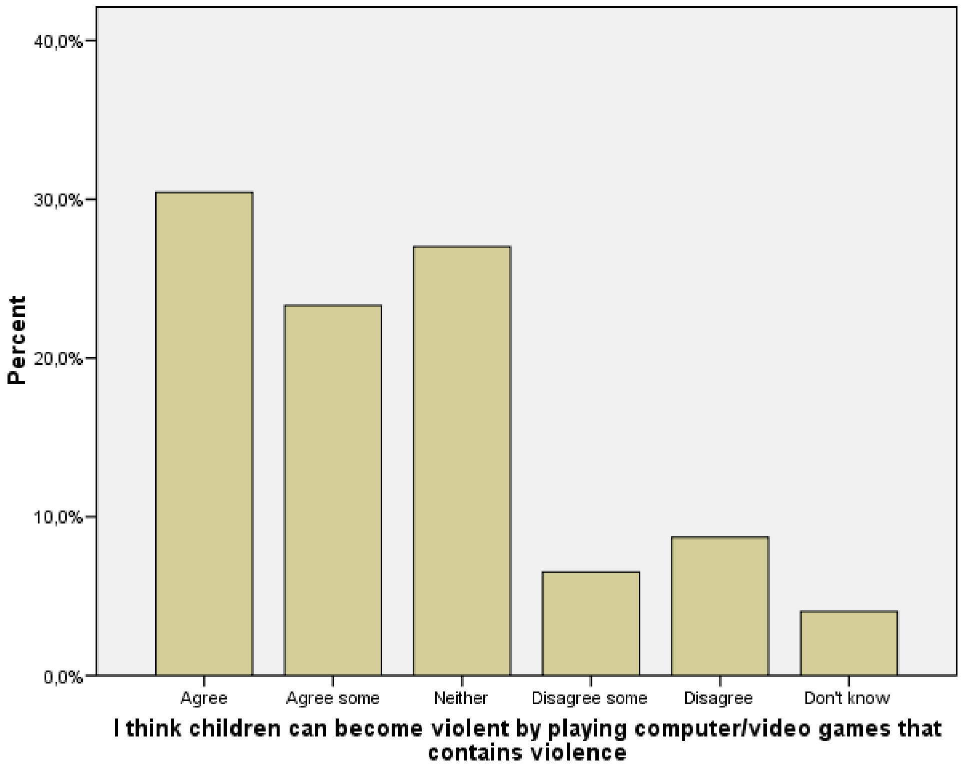

Figure 6: Question 25: I think children can become violent by playing computer/video games that contains violence

where the killers played violent video games before the shootings. But it can also be counter augmented that people who are violent to begin with, will be drawn to violent games.

The American Psychological Association summarizes the issue as

> Psychological research confirms that violent video games can increase children's aggression, but that parents moderate the negative effects. [81]

At the same time some basic statistics about gamers can shed some light on the arguments:

- The average game player is 33 years old and has been playing games for 12 years.
- The average age of the most frequent game buyer is 40 years old. In 2006, 93 percent of computer game buyers and 83 percent of console game buyers were over the age of 18.

These statistical facts is provided by the Entertainment Software Association [82].

6.5 Question 26

I feel that children rather should be doing sports than playing computer/video games

Question 26 can probably be seen in conjunction with question 23 and question 24. Doing sports is often considered to be a more social act than to play computer and video games. The results from the question can be seen in figure 7.

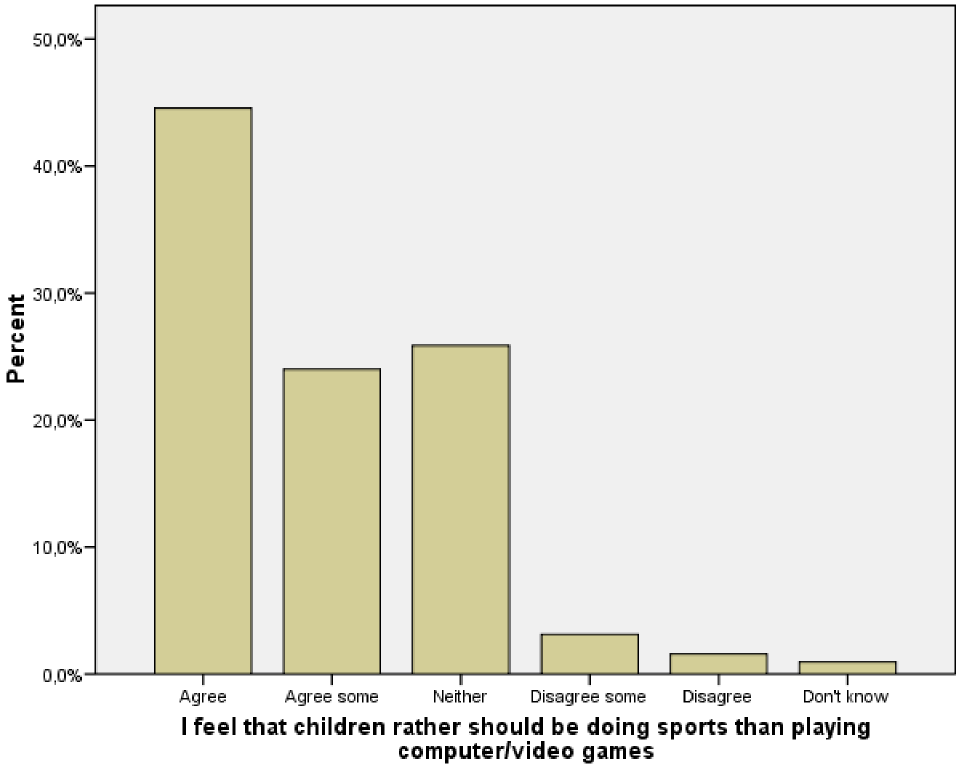

Figure 7: Question 26: I feel that children rather should be doing sports than playing computer/video games

As we see, over 44 % agree and 24 % agree some to the statement that children should rather be doing sports than playing computer or video games. This is somewhat similar to question 23. Approximately 26 % says "neither", and 5 % say they disagree or disagree some.

6.6 Question 27

I think children become inactive by playing computer/video games

Question 27 falls into the same category as question 23, 24 and 26. The results can be seen in figure 8.

As was the case with the questions 23, 24 and 26, a majority answers that they agree. Almost 62 % says they to some degree agree to the statement. 26 % says "neither", while 11 % say they disagree or disagree some.

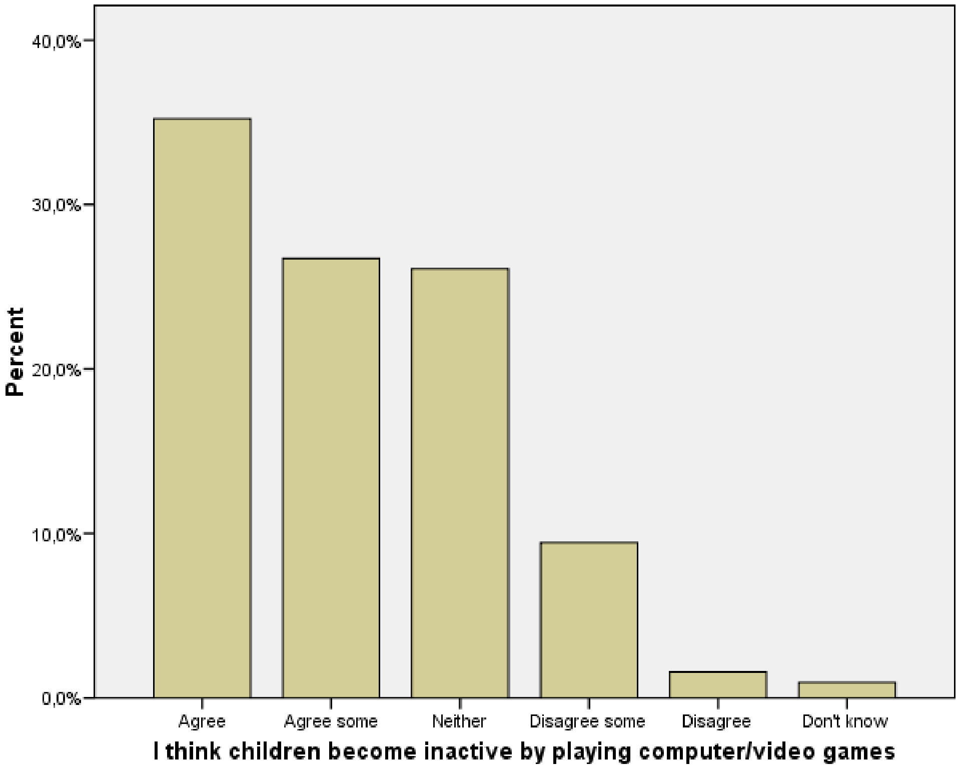

Figure 8: Question 27: I think children become inactive by playing computer/video games

6.7 Question 28

It is smart of adults to play computer/video games with the children, in order to get knowledge of children's use of this medium

As mentioned in connection with violence in computer and video games, it is the opinion of some that parents moderate the potential negative effects. Therefore it could be argued that parents should spend time together with their kids, playing these games. This enables them to explain things so that children better might understand that the violence seen in a game is not real and cannot be applied to the real world. As we saw in the results from question 25, many parents are concerned with violence in video and computer games, so one possible solution are for adults to play together with kids. The results can be seen in figure 9.

Over 43 % agrees to the statement and almost 32 % agrees some. Nearly 17 % says "neither", while a little over 5 % disagrees to some degree. Approximately 3 % says they don't know if it is smart that grownups play together with children.

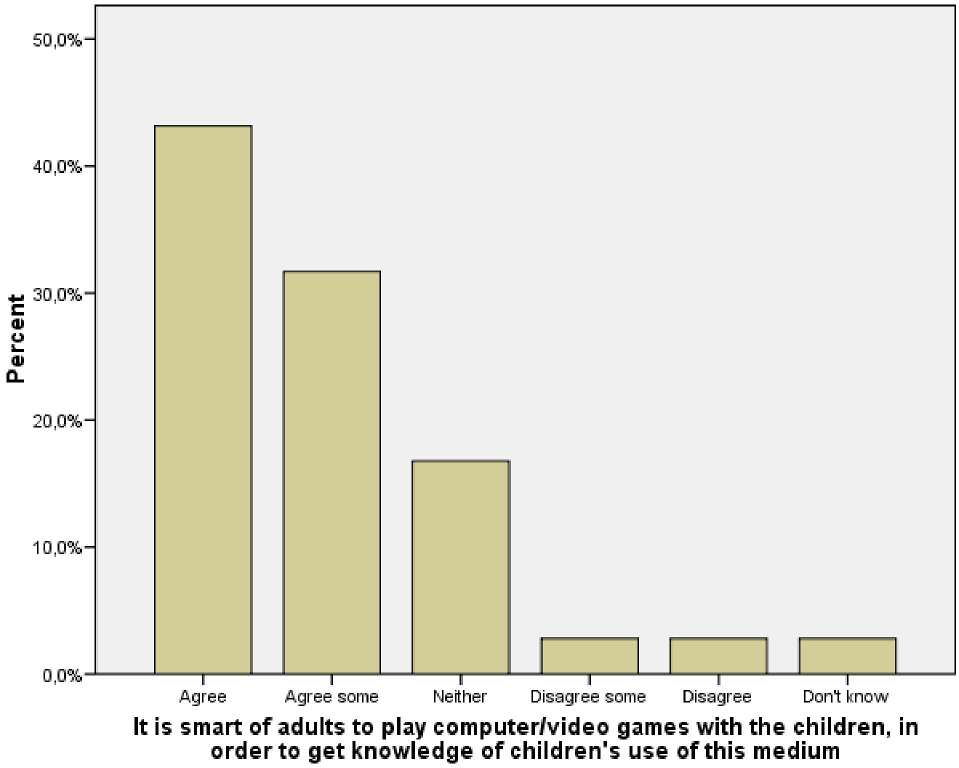

Figure 9: Question 28: It is smart of adults to play computer/video games with the children, in order to get knowledge of children's use of this medium

6.8 Question 29

It is safer for the child(ren) to play on a game console than surfing on the Internet

In question 29 we wanted to find out if parents think it safer to use a game console rather than surfing on the Internet. In retrospect we can see that the question is somewhat ambiguous. We wanted to find out if they thought playing online games is more secure than surfing on the Internet. But we forgot to emphasise the fact that the game console in question is connected to the Internet. This means that the answers we got cannot be used the way we wanted to. The answers we got can be seen in figure 10.

A little more than 54 % agrees somewhat to the statement. About 26 % says "neither", while about 6 % says they disagree or disagree some. 13 % say they don't know. This might be a consequence of the fact that the question is ambiguously defined, or that they simply don't know if it is the case.

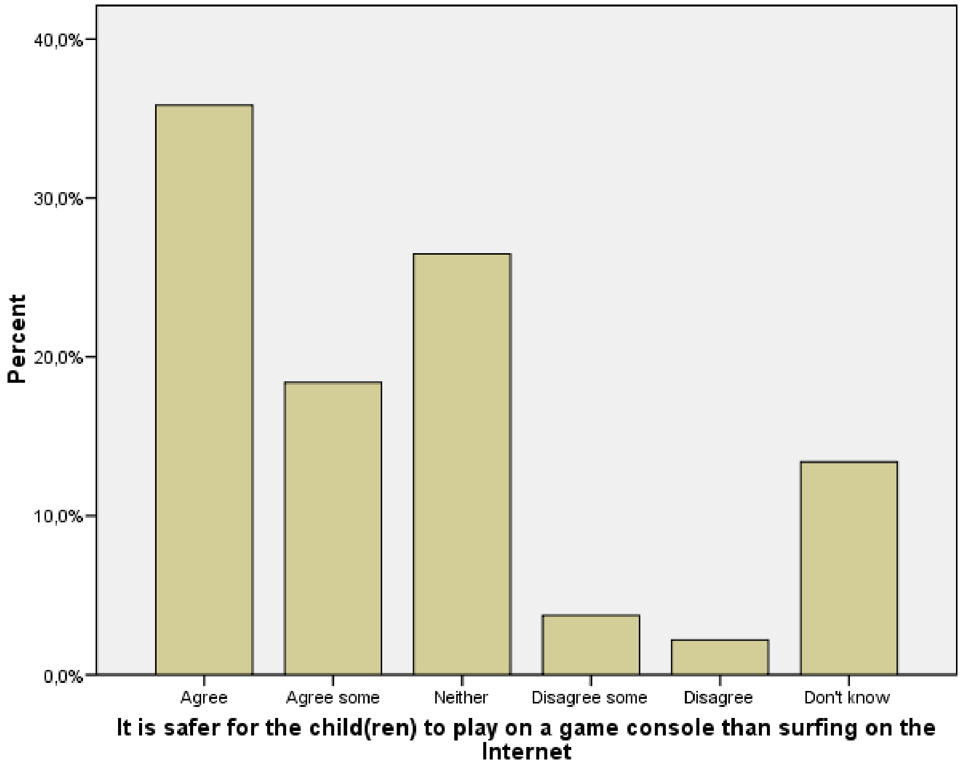

Figure 10: Question 29: It is safer for the child(ren) to play on a game console than surfing on the Internet

6.9 Question 30

Game consoles that are connected to the Internet are a target for virus

Question 30 is a question asked for a different purpose than most of the other questions. This is a question that we don't know the answer to, since there are no reports of viruses targeted against game consoles. But we still wanted to find out if this was the opinion of the owners of game consoles. On the other hand, a question phrased like this might compel the answerer to say that yes, he or she thinks this is the case. If we got a lot of agreeing answers to this question, this might mean that many people think this is the case or that they agree based on the phrasing of the question. The results can be seen in figure 11.

But as we can see from the results, over 60 % say they don't know if this is the case. This means that many people just don't know if a game console connected to the Internet is a target for viruses. About 23 % say that they agree to some degree that this is the case, 11 % says neither while about 4 % say they disagree.

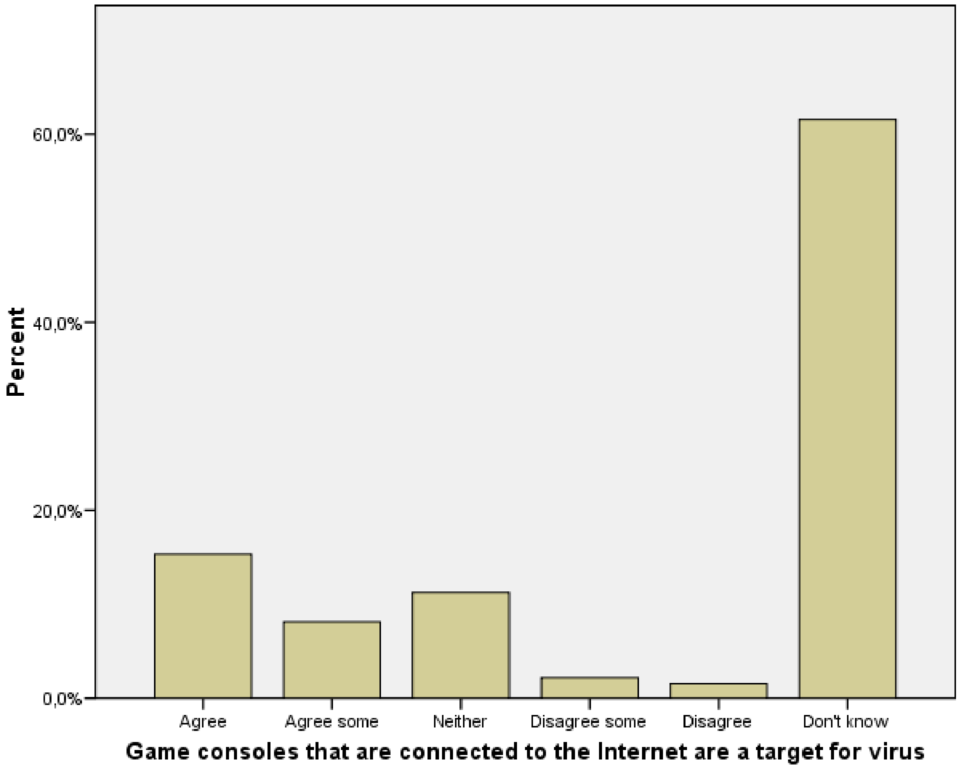

Figure 11: Question 30: Game consoles that are connected to the Internet are a target for virus

6.10 Question 31

We use the built-in possibilities in the game consoles to control what kind of contents the child(ren) has access to

As we have seen over the last decade, and also on question 25, violence in video games is something that is concerning a lot of people all over the world. A lot of research has been done in the area, and legislative means has been put in place. But what very many people do not realise is that the game industry has for several years used a content rating system. These rating system is similar to the system that exists for movies, giving the game a rating which tells the user for what ages the game is suitable. In North America we have the Entertainment Software Rating Board [83], in the European Union we have the Pan European Game Information [84] and in other parts of the world similar systems exist.

The problem with these rating systems is that most people just ignore them. In all modern game consoles today, it is possible for a grown-up to enable these systems. When such systems are enabled, children of a certain age will not be able to play games that are rated unsuitable for them. But it has been proven time and again that parents don't know about these measures, or they don't care, or their children are able to convince them that it is not necessary. The results to the question can be seen in figure 12.

With this question we can again interpret the category "neither" as don't know. There

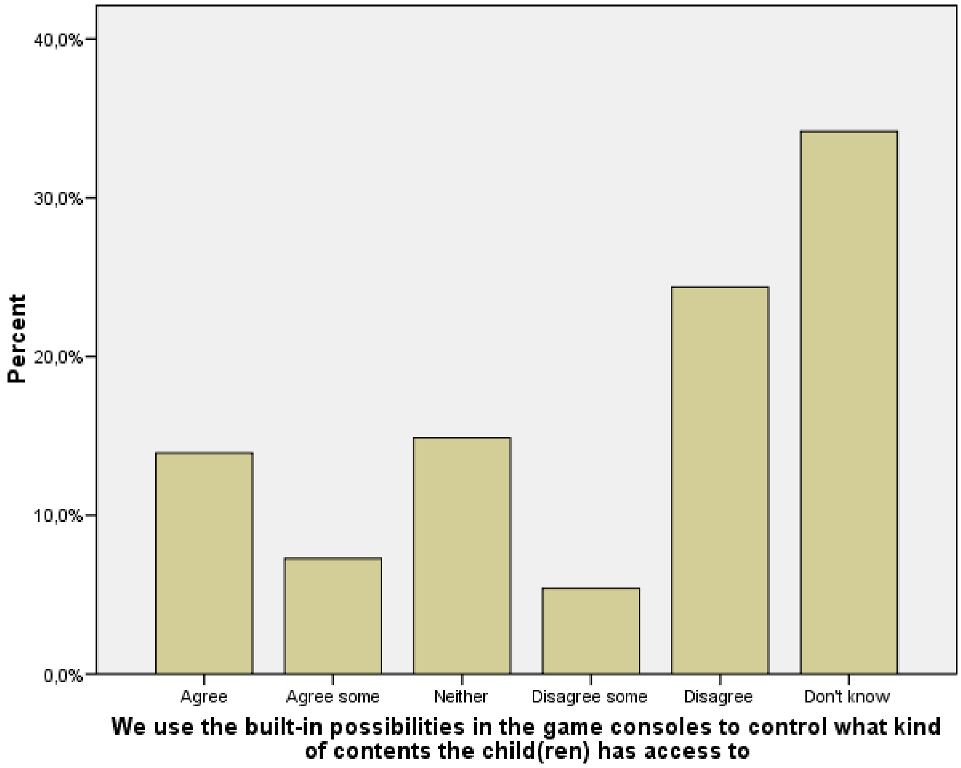

Figure 12: Question 31: We use the built-in possibilities in the game consoles to control what kind of contents the child(ren) has access to

was almost 15 % who answered neither, and a little over 34 % who answered "don't know", giving us a total of 49 % who don't know if they use these measures. 14 % agree, 7 % agree some, 5 % disagree some and over 24 % disagree. These numbers stands in stark contrasts to the results from question 25, where parents expressed a concern about video game violence. If this is the case then they should probably try to use the measures provided by the game industry to protect their children from unwanted content.

6.11 Game console statistics

As part of the questionnaire we asked what kind of game consoles people have. It is interesting to see how many network enabled consoles that has made it out into peoples homes. This can give us and indication of how vulnerable kids might be in regards to online gaming on a game console. A simple frequency analysis is presented in figure 13.

We clearly see that it is the PlayStation 2, together with the computer, that dominates people's use of game platforms. After this come Nintendo's handheld game consoles, the GameBoy and the DS. It is clear that in this group of users, the change from the sixth to the seventh generation of game consoles has not been large. This means that most of the game consoles that this group of user has access to are not network enabled, not counting the computer. But this will change over time, as more and more people opt for a new game console.

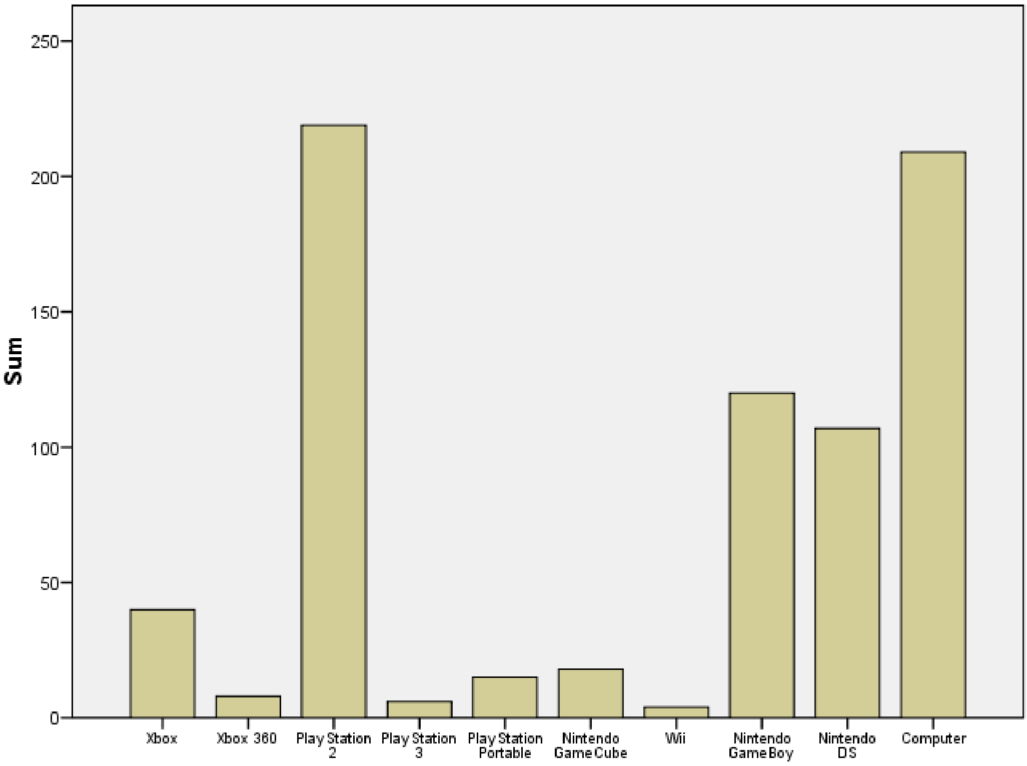

Figure 13: Game console statistics

6.12 Indexes

When we finished the basic frequency analysis of the questions that interested us, we started creating some indexes. The purpose of this is to try and see if we see a change in the answers we got, if we compare them together with other information that we gathered. Some of these indexes are more elaborate than others.

6.12.1 Network enabled consoles

Out of all the consoles that were listed as options in the survey, some of them have built in capabilities of online connectivity. These are the Xbox, Xbox 360, PlayStation 3, PlayStation Portable, Nintendo Wii and Nintendo DS. The PlayStation 2 has been omitted since it requires on of the newer versions of the console to have built in network capabilities. A frequency count of these consoles can be seen in figure 14.

As we see, 54 % have no consoles that are network enabled. 36 % have one console, 9 % have two and below 1 % have three. What we want to do with this statistic is to compare it with question 3: "We have game consoles that are connected to the Internet". A frequency count of this question can be seen in figure 15.

As we see from the figure, 83 % say "no", 12 % say "yes" and 5 % say "don't know".

What we wanted to find out is whether or not those who answer that they don't have a game console connected to the Internet, has consoles that can be connected. Out of those who answered "no" on the question if they have game consoles connected to the Internet, 56 % have zero consoles that can be connected to the Internet. About 36 %

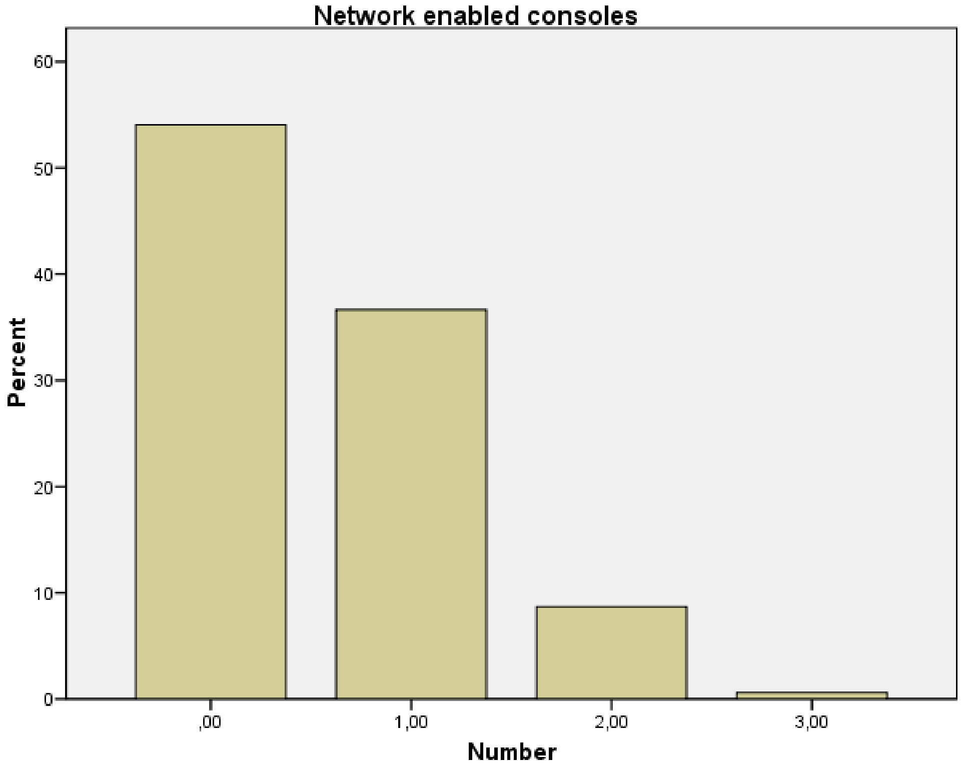

Figure 14: Network enabled consoles

have one console that can be connected to the Internet and 7 % have two consoles that can be connected to the Internet.

Of those who answered that they don't know if they have game consoles that are connected to the Internet, 69 % have zero consoles that can be connected to the Internet. 31 % have one console that can be connected to the Internet, and no one has two or three consoles that can be connected to the Internet.

It can be speculated if those who answer "no" on the question really know if there are game consoles that are online in the home. About 43 % of these has one or more console that can be connected to the Internet. And some of these consoles are really easy to connect. All we really need is an unsecured WLAN, and we are connected. We like to think that the parents are aware if their children has connected a game console to the Internet, but this might not always be the case. Of those who say they don't know if they have a console that is connected to the Internet, 31 % have a console that can be connected. Again we can argue that if they don't know, it might be the case. Children is often more versed in the use of technology than their parents are, and with the ease of how game consoles can be connected to the Internet it is not a far stretch to imagine that a game console can be connected without the parents realising it. It might also be the case that the parents does not even realise that the game console can be connected to the Internet.

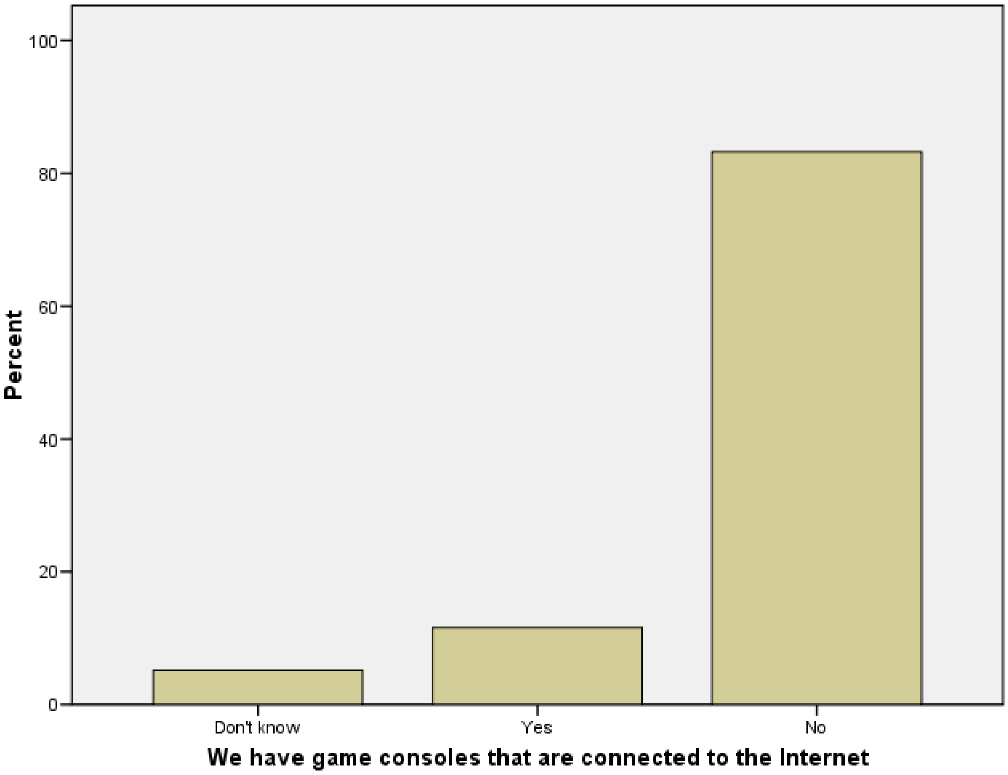

Figure 15: Question 3: We have game consoles that are connected to the Internet

6.12.2 Negativity index

The first index we created we have called a negativity index. This index is meant to tell how negative the person who answers the questions is to computer and video games. For this purpose we picked the following questions:

- Question 23. I feel that playing computer/video games on the Internet is unsocial
- Question 24. I feel that it is smart to limit children's time usage when it comes to playing computer and video games
- Question 25. I think children can become violent by playing computer/video games that contains violence
- Question 26. I feel that children rather should be doing sports than playing computer/video games
- Question 27. I think children become inactive by playing computer/video games

All these questions are negatively formulated questions, meaning that the more negative we are to the given statement the lower the score. But in order to make the index more understandable, we flipped the scale around. This means that the index should give us a score between 5 and 25, and the higher the score we get the more negative the person is to video and computer games. But in reality we also get scores that is lower than 5, since there are people who didn't answer all of the questions. The frequency count of this question can be seen in figure 16.

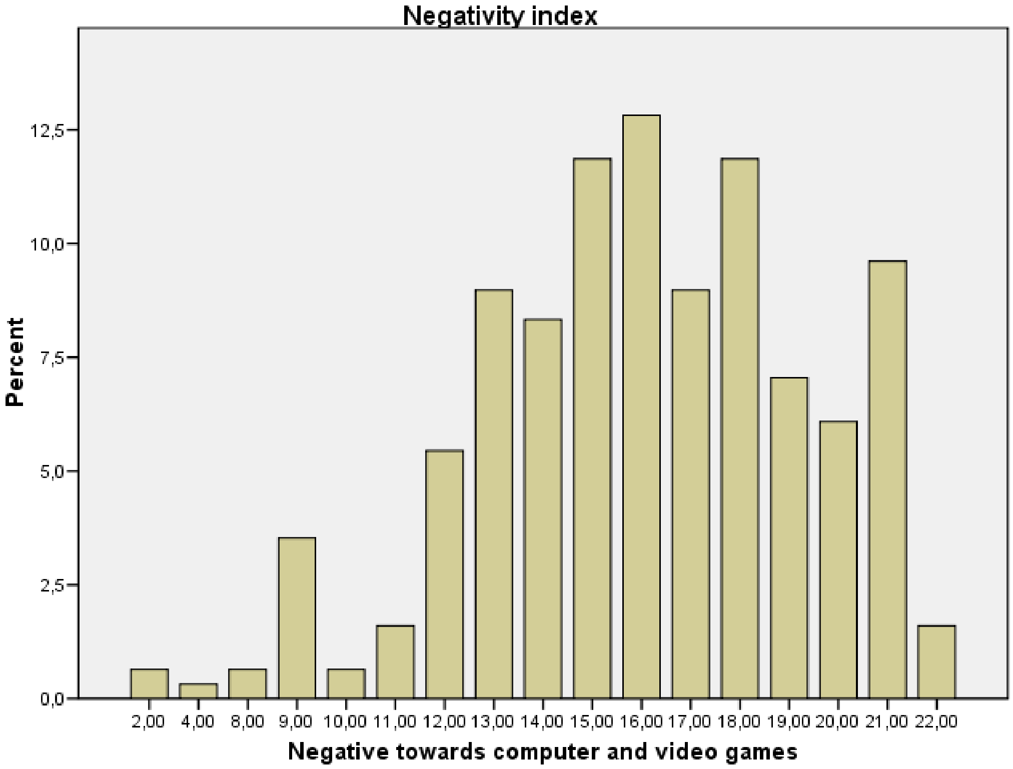

Figure 16: Negativity towards computer and video games

Since the scale we created should be between 5 and 25, we would expect an average value of 15. The mean value of our index is 16. This means that the mass of the distribution of data is slightly shifted towards the right side of the figure. This gives rise to a suspicion that there are more people who are negative towards video and computer games, than there are people who are positive.

The goal of this index is to use the values we find, and check them up against the other questions we asked about games and game consoles. Here it is important that we don't use the index to check against the questions that the index is based on, since this can create some unintended consequences in our results. We have therefore only checked this index against questions 28 through 31.

Analyses of variance (ANOVA) was used to look for systematic variation on the index caused by the questions. The index has been used as the dependent variable, and the questions as the independent variables. Out of the four questions, three of them have significance difference in the negativity towards games index.

Question 29. It is safer for the child(ren) to play on a game console than surfing on the Internet. As has been mentioned before, this question was formulated wrong in accordance with the answers that we wanted to achieve. We wanted to ask it the answerer thought that it is safer to play online on a game console than surfing on the Internet. But the question lacks the clarification that it is about online gaming. We see from the ANOVA that as we move from the agree side of the scale, towards the disagree side of the scale, people become less negative towards games and consoles. In other words, the more people agree to the statement that it is safer to play on a console than surfing online, the more negative they become towards games.

This might seem a contradiction, since those who are negative against game consoles might be expected to disagree with the statement. But since the question is formulated in a way we didn't intend, it might be seen as a choice between to evil, and that the game console is the lesser of the two.

Question 30. Game consoles that are connected to the Internet are a target for virus. This question is one that we really don't have an answer to, since there are no reported incidents of viruses in the wild that targets game consoles. But it still is interesting to see what people think. As we move from the agree side of the scale, towards the disagree side the people answering become less negative towards games. In other words, the more we disagree to the statement that game consoles are a target for viruses, the less negative we are towards games and game consoles.

Question 31. We use the built-in possibilities in the game consoles to control what kind of contents the child(ren) has access to. With this question we se a change in the answers when compared to what we saw in figure 12. In the original frequency count we had a top in the agree, neither and disagree categories. But when we adjust with the negativity index, we have tops at the agree and disagree sides of the scale, and lower scores in the middle range. This means that those who answer on the agree and disagree sides of the scale are prone to be more negative towards games. The ones who answer in the middle of the scale seem to be less negative towards games.

6.12.3 Vulnerability index

Another index we created is a vulnerability index. This index indicates how vulnerable the person answering is when using the Internet. It can indicate vulnerability towards several different things. The questions the index is based on are:

- Question 4. We use a firewall on our computer
- Question 5. We use antivirus on our computer
- Question 9. I have written down passwords because there are too many to remember
- Question 10. I use the same password for several services
- Question 11. Children should have the possibility of using the Internet without adult supervision
- Question 15. Netiquette is a subject that has been discussed with the child(ren) at home
- Question 16. Netiquette is a subject that the child(ren) learn in school

- Question 17. Netiquette is a subject that has been discussed in regards to game worlds and virtual worlds on the Internet
- Question 31. We use the built-in possibilities in the game consoles to control what kind of contents the child(ren) has access to

As was the case with the negativity index, we had to adjust some of the data in order to create a good index. Most of the questions are based on a value between 1 and 5. But some of the questions are negatively formulated, giving low scores when we agree and high score when we disagree. Other questions are positively formulated, giving high scores when we agree, and low scores when we disagree. Because of this, the scale on question 9, 10 and 11 has been flipped. Question 4 and 5 does not fit this pattern; they are "yes", "no" and "don't know" questions. These have also been altered to fit into the index. "Yes" has been assigned the value 1, "No" has been assigned the value 3, and "don't know" has been assigned the value 5. This gives us an index that has values between 9 and 45, and the higher the score the more vulnerable we are. Figure 17 gives a frequency count of the index.

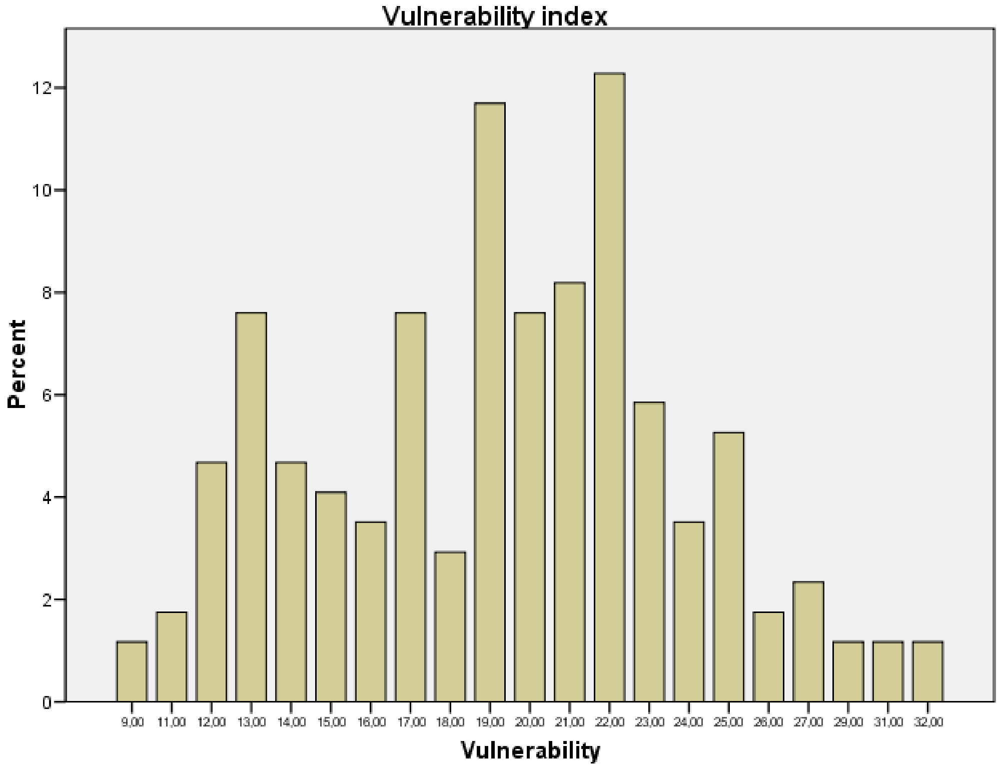

Figure 17: Vulnerability index

As we see from the figure, there was no one who scored close to the maximum score. The highest score is 32, with 45 being the max score. There is a slight shift towards the left side of the figure. There are seemingly more people in the less vulnerable category, than in the more vulnerable category.

We use this index against the game questions in the survey (questions 23-31). This was done in order to see if we could find any significant differences between the people considered to be vulnerable and those who are considered less vulnerable.

Question 25. I think children can become violent by playing computer/video games that contains violence. The question about violence in video and computer games has a significant change when we adjust with the vulnerability index. The more people agree with the statement, the less vulnerable they are. This means that when we move towards the disagree part of the scale; the people answering become more vulnerable. This gives rise to believe that the less vulnerable people might know more about computer and video games, and therefore tend to agree to the statement.

Question 29. It is safer for the child(ren) to play on a game console than surfing on the Internet. As has been mentioned before, this question is formulated differently than what we intended. But none the less, we see a significant difference within the vulnerability index. As we move from the agree part of the scale, towards the disagree part of the scale, the vulnerability index score rises. This means that the people agreeing to the statement are less vulnerable than the people who disagree.

Question 30. Game consoles that are connected to the Internet are a target for virus. As is the case with the other two questions, in question 30 we also see a significant change when we adjust with the vulnerability index. Again the people who agree with the statement are less vulnerable than the people who disagree. But this question received a remarkable high amount of "don't know" answers as was seen in figure 11. This could make the statistics somewhat skewed. And at the same time, there is really not an answer to this question at the time of writing. But it would seem that the people who believe that a game console is a target for viruses, is also less vulnerable in general.

The last question, number 31, has been omitted from this test. This is done because the vulnerability index bases itself in part on this question. And checking a question against an index that is partly based on that question can give us some strange results.

6.12.4 Own computer usage

As part of the background information, we asked the person filling out the questionnaire what that person usually used in regards to computer and Internet technology. The possible answers were:

- Uses computer at work
- Uses Internet at work
- Uses computer at home
- Uses Internet at home
- Uses e-mail
- Uses online chat
- Plays computer/video games

Based on these answers we created an index over the person filling out the questionnaires own computer usage. Since the questions should be answered through a checkbox, we have interpreted a blank box as a "no" answer. "Yes" has been given the value 1, and "no" have been given the value 0. This gives us a value between 0 and 7. A frequency count of the index can be seen in figure 18.

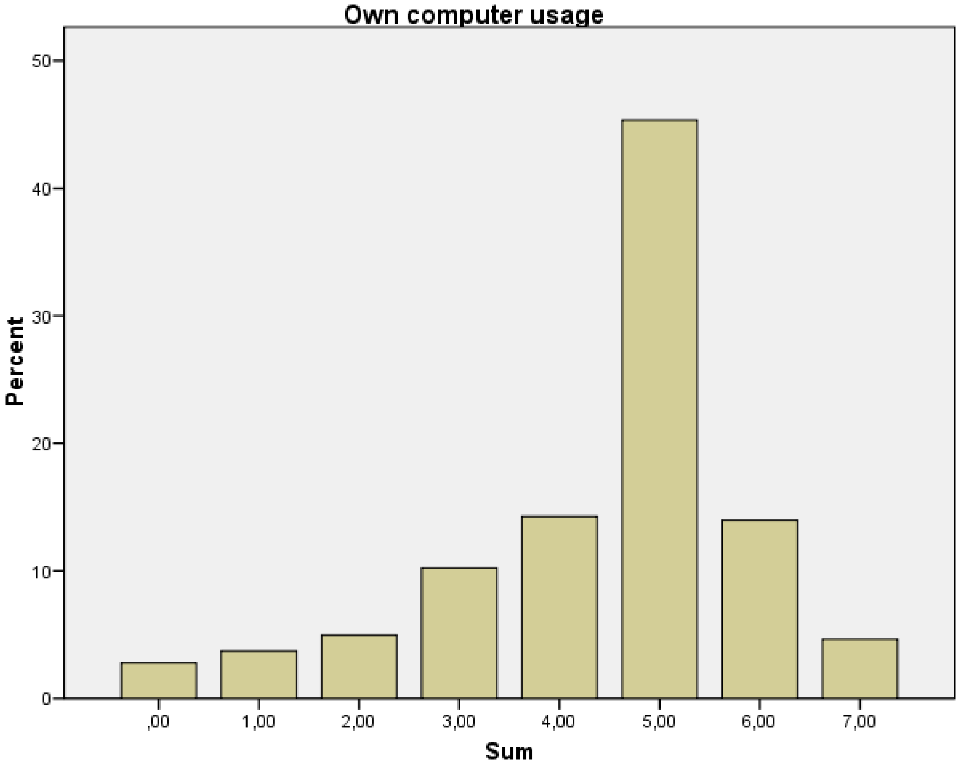

Figure 18: Own computer usage

As we can see from the figure, the most common score (45 %) is 5. It is the first five alternatives that are the most frequently filled out. This gives us an indication that it is quite common to use computers and the Internet amongst the people answering the survey.

We checked this index against the game questions in the survey (questions 23-31). We did this in order to see if there is a difference in attitude towards games and game consoles between the people who use computers a lot and people who doesn't.

Question 23. I feel that playing computer/video games on the Internet is unsocial. As we saw in figure 4, there was a large number who agreed to the statement, and a large number who answered in the "neither" category. But when we check the question against the "own computer usage" index, the groupings change. It is now more centred on the middle of the scale. So it would seem that the more the person answering the questionnaire uses computers and the Internet, the more he or she leans towards a more moderate view. They are more inclined to disagree on the question if playing games online is unsocial.

Question 25. I think children can become violent by playing computer/video games that contains violence. We see the same kind of trend with question 25, as we saw with question 23. When we adjust the results we found in figure 6 with the person answering own computer and Internet usage, we see a moderating trend here too. The higher the person scores on the "own computer usage" index, the more he or she is inclined to disagree that children playing violent computer and video games can become violent. As was the case with question 23, there is also here a more centralisation of the data around the three middle categories.

6.12.5 Own video and computer game usage

One connection we wanted to investigate is whether or not there is any difference between people who play games, and those who don't. So we conducted a T test, with the questions about games (23-31) as test variables. Then we used the yes/no question asking if the person filling out the questionnaire play games, as a grouping variable. This test gave us the results that in 3 out of the 9 questions there was a significant difference between those who play games and those who don't.

Question 24. I feel that it is smart to limit children's time usage when it comes to playing computer and video games. As we saw in figure 5, more than 90 % of the answers agrees with this statement. Therefore there is little in the way of differences to be found between those who play and those who don't. This can also be seen when we look at the mean values of the two groups. There is not a big difference between the group that plays video and computer games, and thos who don't. And when more than 90 % agrees with the statement, there is really little to be gained from this analysis.

Question 28. It is smart of adults to play computer/video games with the children, in order to get knowledge of children's use of this medium. With this question, we want to see if people who play games agree more often than those who don't play that it is smart for adults to play together with their children. Approximately 75 % says that they agree to the statement to some degree. Again we see that the predominance of answers agrees to the statement, making it difficult to say if there is a real different between those who play games and those who don't.

Question 29. It is safer for the child(ren) to play on a game console than surfing on the Internet. As has been mentioned before, there is a problem with the wording of this question. What we wanted to ask was if people think it is safer to play online on a game console, rather than surfing online. So the question doesn't really concern the problem we wanted it to. But there is a significant difference between people who play and those who don't when using the question as it is.

As we saw in figure 10, there is more uncertainty in the answers to this questions than what it was with the first two. The T test gives us results that indicate that there is a significant difference between those who play and those who don't. This question is stated in such a way that if we agree we get a low score, but if we disagree we get a high score. The people who play games are more inclined to disagree with the statement.

7 Discussion and conclusions

7.1 Discussion

All the consoles we have tested seem to have some sort of security measures implemented. The Xbox Live system is the one that takes it the furthest, by authenticating and encrypting all traffic. The PlayStation 2 has a built-in function that shuts down the network interface when it is not needed, making it impossible to reach it over the network. The Wii encrypts traffic that is considered to sensitive. It also releases its IP address when it is not needed, making it more difficult to reach it over the network. Both the Nintendo DS and the PlayStation Portable does the same. Whether or not these functions were implemented with security in mind does not really matter, they work in favour of it anyhow.

We did find indications that a game console is attackable over the Internet in the same way that a computer is. We found a known vulnerability in the Wii, and some other things in some of the other consoles. This could also open up for building botnets with game consoles, infecting them with worms or viruses, using them to send spam and so on. But game consoles are different than computers in the sense that they are easier to control for the manufacturers. They have full control over both the hardware and the software, together with the services provided for the platform. This might make it easier to protect a game console from many of the known problems in the computer world. And it can also be argued that few people will take the time and resources needed to develop a new virus or worm for a game consoles, when there are so many more accessible systems out there.

We also did some testing on modified a Xbox. The software on the console that we tested has known security vulnerabilities, and has had so for several years. There are no fix for the problem, and there probably will not be one. This is one of the problems with using modified game consoles and software provided by unofficial sources. There is no guarantee that security problems will be fixed, since the programming often is done on an ad-hoc basis by crackers or hackers. If such security vulnerabilities had been discovered in official software they would be fixed as fast as possible, at least in order to avoid bad publicity. It should however be noted that the Xbox is out of production, and this might explain why new software is not released.

The tools we have used in our technical experiments are widely known and distributed for free on the Internet. They have been able to discover some interesting things about the consoles in question, and also detect and confirm some vulnerabilities. On the other hand we see that they often get confused when turned against game consoles. They are not quite sure what they are up against, and therefore the results have to be interpreted with this in mind.

When it came to the questionnaire we found some interesting results. The listing of what type of game consoles people have, showed that it is still dominated by the sixth generation. Especially the PlayStation 2 is very widespread. Together with this it is common to use computers and the handheld consoles from Nintendo. But this will inevitably change as people switch to the new generation of consoles.

As we have seen, the old perceptions about computer and video games still live strong. Parents feel that their children can become violent by playing violent games. Whether or not this is true is difficult to say. The experts in this field dispute on the topic. At the same time we see that many parents are not aware of the fact that they can limit children's access to violence. At least on the game consoles. All modern game consoles have the possibility of parental controls, where the parents can limit what is allowed to be played on the console. All the consoles of the seventh generation have this possibility, and some of the sixth generation consoles.

It is still also predominantly believed that playing games makes the player inactive. And in many cases this is probably true. But at the same time, new concepts such as EyeToy, Dance Dance Revolution and Nintendo Wii make sure that the player has to move in order to play. As we see more and more of such concepts, we might see a change in this perception. We also see that it is quite common to feel that children should rather do sports, than play computer and video games. But also here we have seen some changes the latest years. Dance Dance Revolution has become a sport all of its own, with championships carried out all over the world.

There are some measures that are popular, or that works to mitigate the potential damages that can come from playing games. Adults playing together with their children, making sure that children understand what are going on and explaining things. This has been seen to mitigate the potential risks from playing violent games. Many also feels that it is smart to limit the children's time spent playing games. This might be seen in conjunction with the fact that many see online gaming as an unsocial and sedentary activity. But again there are exceptions, with games that forces the player to interact with other players in order to survive, or concepts that makes the player move during game play.

When we conducted a deeper analysis of our survey data, we discovered that there is little difference between those who play themselves, and those who don't. They more or less agree to the same things. We did however discover that the more a person uses computer and Internet technology, some answers shifts. When answering the questions about violence in computer games, and if it is unsocial to play online, the more that person uses computers and Internet, the less they agree. This means that people using computer and Internet often, seems to feel less negative towards playing games online and games with violence.

During our analysis of the survey data, we also constructed several indexes. We used these indexes against some of the questions, to see if we could find any connections between certain types of answers. The negativity index that we created bases itself on most of the questions about games and game consoles, and can therefore not be applied to the same questions that it is based on. But we applied it to the other questions about games, and found some interesting results. The answers to the questions about parental control shifts when we adjust with the negativity scale. The people answering on the agree or disagree side of the scale, tend to be more negative towards games, while those answering on the middle of the scale tend to be less negative. This could be because the people who are less negative also are less prone to look for solutions to protect their children, and therefore answers more in the middle of the scale. Or it might be that they haven't considered every measure that can be taken, and therefore answers with less certainty.

Another index that we created was a vulnerability index. This index bases itself on various questions from the questionnaire. When applied to the questions about games we see that people who are less vulnerable tend to agree to the statement that children might become violent by playing violent games. This might stem from the fact that the less vulnerable knows more about computers and games in general and therefore have a stronger feeling that violent computer and video games might affect their children.

We also did some analysis around the consoles that can be connected to the Internet. We used the question if the person answering has a game console connected to the Internet, and checked if that person stated that he or she had consoles that could be connected to the Internet. Out of all those who said that, no they didn't have a console connected to the Internet, more than 40 % say they have a console that can be connected. This is not to say that they didn't answer truthfully, but it is often the case that children know more about the technology than their parents. If this is the case, then it is possible that they have connected the console to the Internet without the knowledge of the parents. Especially in the case of the consoles that support WLAN, this is a very simple task.

7.2 Conclusions

Here we return to the original research questions and try to answer them.

Does the installation of a new game console in the home open for new vulnerabilities that we are not aware of?

This would seem to be a possibility. As the game consoles evolve and become increasingly more like a computer, the complexity of it also increases. The potential for vulnerabilities becomes bigger the more complex the software is. We did discover a vulnerability in the Nintendo Wii, and there probably is similar undiscovered vulnerabilities in other game consoles.

Are there more potential vulnerabilities in a console that has been modified, than in an unmodified console?

The modified console we tested was an Xbox. The software that we tested has had known vulnerabilities for several years, without a fix being made available. The potential problem with a modified consoles running homebrew software is that it is not supported by the manufacturer, and the software is often made available in an ad-hoc fashion. There is no review of the code, and there is no official apparatus to take care of such incidents. If there are more potential vulnerabilities in a modified console versus and unmodified one, is difficult to answer. But the unmodified one has a official system that updates and fixes bugs and vulnerabilities, as opposed to a modified one where there are no official channels for updates.

Do we need to take special precautions when connecting a new game console to the home network?

At the time of writing there have been no reports of vulnerabilities in game consoles being exploited in the wild. It is not possible to install antivirus or a firewall on a console, with some exceptions. There is all in all little than can be done to protect the game console when connecting it to a network. What is important to remember is to have that same scepticism that we have learned to employ when using the Internet on a computer, and not take everything for granted. If we use a wireless link, it is smart to encrypt it. And always download an install the latest firmware; it might contain security related fixes.

Does users of game and virtual worlds consider their privacy protection in the same way they do when using other services on the Internet?

We have targeted one of the most vulnerable groups of users in our research, kids. When it comes to virtual worlds and games, many parents are sceptical. They are concerned about violence, about kids using too much time playing, kids becoming inactive or unsocial. Many parents say they have taught their children netiquette in one way or another. But it should still be stressed that this also needs to include games and game consoles. They are often considered to be a toy, but in reality they are more and more becoming a communication device like a computer.

Most modern game consoles have some security measures incorporated into them. These are measures that the average user is not aware of, but they are still there. We have seen during this project that it is possible to find vulnerabilities on a game console, even by using freely available tools. This could open up for a new world of malware written specifically for game consoles. We have also seen some indications that software on modified game consoles might be less secure than officially supported software. But the biggest problem is that there is no infrastructure for updating this software, as is the case with the official software.

We have also seen that many parents are concerned about their children's use of video and computer games. This concern can probably be mitigated by the parents themselves. By getting more involved in the children's usage of games, and playing together with the children, many of the potential worrisome aspects can be mitigated. At the same time children should be taught the same rules and netiquette in regards to games and online gaming as they are taught about using the Internet.

8 Further work

8.1 Chapter summary

This chapter presents further ideas to continued work with the material presented in this paper, or other potential projects that was though of during the project period. Some ideas base themselves on this work, while others would be completely new areas of research.

- Most of the game console of today has the possibility of playing old games from other systems. This backward compatibility mode is a way for the game console manufacturers to make the transition from one generation to the next easier, by allowing people with games from the old system to play them on the new one. Does this make the console behave differently? Does it behave differently when interacting with the Internet? Does this open up for vulnerabilities from the old system?
- How common is cheating on game consoles? In the computer world cheating is something that has been around for a long time. But with game consoles, the game manufacturers control both the game and the medium on which it is played. Does this make it more difficult to cheat when playing on a game console, than on a computer? Are there known cases of cheating on modern game consoles?
- Conduct a survey amongst game producers, game developers, game console manufacturers and so on to check what kind of security measurers they take. How do they secure their games and the hardware?
- Information gleaning. Take a look at several games at different platforms and determine what kind of information can be used for cheating or reflex augmentation by analyzing the network traffic.
- Information gleaning. Take a look at one game used on several different platforms, and determine what kind of information can be used for cheating or reflex augmentation by analyzing the network traffic. Are there differences between the same game played on different gaming platforms?
- Reflex augmentation detection. Take a look at whether or not it is possible to detect that network traffic has been altered as part of cheating. This requires that the traffic is not encrypted and/or authenticated, as is the case with the Xbox Live service.
- Do a survey among children to balance the answers we found from parents, in order to see if the parents and children answer the same. If there is a large gap between the answers that the children gives, and the answer that their parents gave, there might be something wrong with the way the parents/schools try to teach children about personal privacy on the Internet. Or they are just not getting through to the children.
- Take a closer look at the security in the different online services that Microsoft, Sony and Nintendo offers. We only took a cursory look at them in this paper. Some of these

systems are very large, and demand a big infrastructure. It can be difficult to easily get a big picture of how they work, seen from the crackers point of view. It might be beneficial to look at only one of the systems.

- Are such systems possible to reverse engineer? Is it possible to emulate the systems in such a way as to able to offer the same services as the original service? This happened with Blizzards Battle.net service [85]. A group of frustrated programmers were able to reverse engineer Blizzards Battle.net service, and launch their own competing service. Is this possible with other such services?
- Most of the modern game consoles today allow user to browse the Internet via the console. And we know from the computer world that quite a lot of information can be found about a computer, through the use of JavaScript's, cookies and so on [86]. What information can be found about a game console through its Internet browser? Some of these browsers are the same as the ones running on a computer. The Internet browser in the Wii is from Opera. Are these browsers susceptible to the same vulnerabilities as their counterpart in the computer world? It would seem so. In April 2007 a vulnerability in the Opera browser made it possible to remotely crash a Wii that viewed a page with a specially crafted or corrupted JPEG image [87]. Can the browsers of game consoles be used to take over the console remotely?
- It has become quite common over the last years for game developers to add copy protection to their products. Systems such as SafeDisc, SecuROM and StarForce have been added to popular games. But do they work in the intended way? Are they just a nuisance to the legitimate users, while crackers can easily avoid these measures? A survey among the users might give some answers.
- Due to lack of equipment we were not able to monitor console-to-console traffic using wireless technology. Would it be possible to emulate, duplicate or replicate this traffic in order to make a computer simulate a game console? How far is it possible to send wireless console traffic using directional antennas? Can this be used as part of a child grooming scheme?
- Rewrite the questionnaire and conduct it again. We came across several questions that we, after the survey was concluded, considered to be poorly stated or formulated. We also asked several question in the form of "Do you think". It could be interesting to compare these results with a survey that bases its questions on a "Do you do" approach. There might be some differences between what people think is smart, and what they actually do.
- Through our survey we have found that many parents find gaming on the Internet to be unsocial. But in the later years several new concepts has risen. Social gaming is something that probably will become much bigger in the coming years. In online multiplayer games like Battlefield 2, it is impossible to be good without cooperating with your team mates. In some Massive Multiplayer Online Role Playing Game (MMORPG) the whole concept of the game is to interact with the other players. The virtual world Second Life creates a whole new world in which users can interact on many levels. It is also becoming very popular with offline social gaming. Here we have games like Guitar Hero, SingStar and other games that are solely based on a social setting where you play with friends in the same physical location. It could be

interesting to see how users off such games compare to those who have never played them. If there is any significant difference in attitude towards games in the group that play social interaction games and those who don't.

- Do a more comprehensive analysis of the data collected through our survey. We have had a somewhat narrow field of view in this project. But the data collected could be used for more purposes than what we did. It is also possible to correct the answers we got with more background information. We tried correcting for own computer usage, vulnerability and negativity towards games. It could also be possible to correct for age, gender, who answers the survey, education level of the parents, and so on.
- Almost all games that are released today are rated in some way. In Europe we have the Pan-European Game Information ratings and in the US there is the Entertainment Software Rating Board. Both these systems aims to rate a game in order to make sure that game is not played by someone it is not suited for. But it often seems that these systems don't work, or that they are just ignored. Parents don't check if the game is suitable for the child, the child just tells the parents what they want or the person behind the counter does not check the age of the buyer. It could be interesting to see what parents know of these rating systems, if they know they exists and if they use them. At the same time it could be interesting to counterbalance the results from the parents with some results from the children themselves, or from people working in the shops who sell games.

Bibliography

[1] Xbox. http://www.xbox.com/, Last visited June 2007. 2.2

[2] Microsoft. http://www.microsoft.com/, Last visited June 2007. 2.2

[3] PlayStation. http://www.playstation.com/, Last visited June 2007. 2.2

[4] GameCube. http://www.nintendo.com/systemsgcn, Last visited June 2007. 2.2

[5] Xbox-Scene.com. http://www.xbox-scene.com/, Last visited June 2007. 2.2

[6] Xbox Linux. http://www.xbox-linux.org/, Last visited June 2007. 2.2

[7] 17 Mistakes Microsoft Made in the Xbox Security System. http://www.xbox-linux.org/wiki/17_Mistakes_Microsoft_Made_in_the_Xbox_Security_System, Last visited June 2007. 2.2

[8] Vaughan, C. 2004. Xbox security issues and forensic recovery methodology (utilising linux). *Digital Investigation*, 1(3), 165–172. 2.2, 2.3

[9] Heckendorn, B. 2005. *Hacking Video Game Consoles: Turn your old video game systems into awesome new portables*. Wiley. 2.2

[10] Grand, J., Yarusso, A., & Thornton., F. 2004. *Game Console Hacking: Xbox, PlayStation, Nintendo, Game Boy, Atari, & Gamepark 32*. Syngress, 1 edition. 2.2, 4.2.4

[11] Grand, J., Kaplan, D., Thornton, F., Yarusso, A., Barken, L., Kinstle, B., Brown, M., Owad, T., Russell, R., & Haas., J. 2006. *Joe Grand's Best of Hardware, Wireless, & Game Console Hacking*. Syngress, 1 edition. 2.2

[12] Seacord., R. C. 2005. *Secure Coding in C and C++*. The SEI Series in Software Engineering. Addison Wesley Professional, 1 edition. 2.3

[13] Bishop, M. 2003. *Computer Security: Art and Science*. Addison-Wesley, 1 edition. 2.3

[14] Gollman, D. 1999. *Computer Security*. Wiley, 1 edition. 2.3

[15] Kaeo, M. 2004. *Designing Network Security*. Cisco Press, 2 edition. 2.3

[16] Schäfer, G. 2003. *Security in Fixed and Wireless Networks: An Introduction to Securing Data Communications*. Wiley. 2.3

[17] Northcutt, S., Zeltser, L., Winters, S., Fredrick, K. K., & Ritchey, R. W. 2003. *Inside Network Perimeter Security: The Definitiv Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems*. New Riders, 1 edition. 2.3

[18] Microsoft's Red-Ink Game. http://www.businessweek.com/technology/content/nov2005/tc20051122_410710.htm, Last visited June 2007. 2.3

[19] November 2006. PlayStation 3 Offers Supercomputer Performance at PC Pricing, iSuppli's Teardown Analysis Reveals. http://www.isuppli.com/news/default.asp?id=6919, Last visited June 2007. 2.3

[20] Hoglund, G. & Butler, J. 2005. *Rootkits: Subverting the Windows Kernel*. Addison-Wesly, third edition. 2.4

[21] DAEMON TOOLS v4.00 released. http://www.daemon-tools.cc/dtcc/archive/daemon-tools-v4-00-released-t6742.html, Last visited June 2007. 2.4

[22] King, S. T., Chen, P. M., Wang, Y.-M., Verbowski, C., Wang, H. J., & Lorch, J. R. SubVirt: Implementing malware with virtual machines. 2.4

[23] Williams, S., Shalf, J., Oliker, L., Kamil, S., Husbands, P., & Yelick, K. 2006. The potential of the cell processor for scientific computing. In *CF '06: Proceedings of the 3rd conference on Computing frontiers*, 9–20, New York, NY, USA. ACM Press. 2.5

[24] Folding@Home Distributed Computing. http://folding.stanford.edu/, Last visited June 2007. 2.5

[25] Xbox 360 'Folding@home' project a possibility, says Moore. http://www.gamesindustry.biz/content_page.php?aid=24855, Last visited June 2007. 2.5

[26] Raymond, E. S. The Case of the Quake Cheats. http://www.catb.org/~esr/writings/quake-cheats.html, Last visited June 2007, 1999. 2.7

[27] Yan, J. J. & Choi, H.-J. 2002. Security Issues in Online Games. *The Electronic Library*, 20, No 2. 2.7, 1, 3, 2.7

[28] Yan, J. J. 2003. Security Design in Online Games. In *ACSAC*, 286–297. IEEE Computer Society. 2.7

[29] Smed, J., Kaukoranta, T., & Hakonen, H. September 20th 2001. Aspects of networking in multiplayer computer games. 2.7, 4, 5

[30] Smed, J., Kaukoranta, T., & Hakonen, H. A review on networking and multiplayer computer games. Technical Report 454, Turku Centre for Computer Science, April 2002. 2.7

[31] IGE. http://www.ige.com/, Last visited June 2007. 2

[32] The Real Price of Virtual Gold. http://www.mtv.com/overdrive/?name=news&id=1545907, Last visited June 2007. 2

[33] Wireshark. http://www.wireshark.org/, Last visited June 2007. 3, 4.3.3

[34] Microsoft. Xbox Rewards: Take Your Gaming to the Next Level. http://www.xbox.com/en-US/community/news/2007/0205-xboxrewards.htm, Last visited June 2007. 2.7

[35] Second Life. http://www.secondlife.com/, Last visited June 2007. 2.7

[36] Chambers, C., chang Feng, W., chi Feng, W., & Saha, D. 2005. Mitigating information exposure to cheaters in real-time strategy games. In *NOSSDAV '05: Proceedings of the international workshop on Network and operating systems support for digital audio and video*, 7–12, New York, NY, USA. ACM Press. 2.7

[37] DeLap, M., Knutsson, B., Lu, H., Sokolsky, O., Sammapun, U., Lee, I., & Tsarouchis, C. 2004. Is runtime verification applicable to cheat detection? In *NetGames '04: Proceedings of 3rd ACM SIGCOMM workshop on Network and system support for games*, 134–138, New York, NY, USA. ACM Press. 2.7

[38] XNA Developer Center. http://msdn.microsoft.com/xna/, Last visited June 2007. 2.8

[39] Jackson, M. January 2007. Nintendo to offer original game downloads for Wii. Computer and Video Games Magazine. http://www.computerandvideogames.com/article.php?id=156286, Last visted June 2007. 2.8

[40] Nintendo's WiiWare Paves the Way for Fresh Games, Cool Consumer Experiences. http://www.nintendo.com/newsarticle?articleid=lJUgYjCGf4pVbYMAU2qmwF3wp7DiOK5k&page, Last visited June 2007. 2.8

[41] February 2007. Xbox 360 Hypervisor Privilege Escalation Vulnerability. http://www.securityfocus.com/archive/1/461489/30/0/threaded, Last visited June 2007. 2.8

[42] Nintendo DS: More Than A Gaming System? http://www.myfoxmilwaukee.com/myfox/pages/Home/Detail?contentId=2311167&version=4&locale=EN-US&layoutCode=VSTY&pageId=1.1.1, Last visited June 2007. 2.9

[43] Leedy, P. D. & Ormond, J. E. 2005. *Practical Research - Planning and Design*. Pearson Merrill Prentice Hall, 8th edition. 3.1

[44] Sony Computer Entertainment Inc. Business Data Cumulative Production Shipments of Hardware / PlayStation®2. http://www.scei.co.jp/corporate/data/bizdataps2_e.html, Last visited June 2007. 4.2.1

[45] PC Vs Console - PlayStation 2 Technical Specifications. http://www.pcvsconsole.com/features/consoles/playstation2.php, Last visited June 2007. 4.2.1

[46] Wikipedia - PlayStation 2. http://en.wikipedia.org/wiki/PlayStation_2, Last visited June 2007. 4.2.1

[47] Sony PlayStation 2 Specs. Consoles Specifications. http://reviews.cnet.com/Sony_PlayStation_2/4507-6464_7-30012264.html, Last visited June 2007. 4.2.1

[48] Sony Computer Entertainment Inc. to launch its next generation computer entertainment system, PlayStation 3 in spring 2006. http://www.scei.co.jp/corporate/release/pdf/050517e.pdf, Last visited June 2007. 4.2.2

[49] Sony PlayStation 3 (60GB) Specs. Consoles Specifications. http://reviews.cnet.com/Sony_PlayStation_3_60GB/4507-10109_7-31355103.html?tag=sub, Last visited June 2007. 4.2.2

[50] About PlayStation 3 - Technical Specifications. http://www.us.playstation.com/PS3/About/TechnicalSpecifications, Last visited June 2007. 4.2.2

[51] Sony PSP Specs. Consoles Specifications. http://reviews.cnet.com/Sony_PSP/4507-10109_7-30895581.html?tag=sub, Last visited June 2007. 4.2.3

[52] PlayStation Portable - About PSP - techspecs. http://www.us.playstation.com/psp/about/techspecs, Last visited June 2007. 4.2.3

[53] Microsoft Xbox Specs. Video Game Consoles Specifications. http://reviews.cnet.com/Microsoft_Xbox/4507-6464_7-7853769.html, Last visited June 2007. 4.2.4

[54] PC Vs Console - Xbox Technical Specifications. http://www.pcvsconsole.com/features/consoles/xbox.php, Last visited June 2007. 4.2.4

[55] Wikipedia - Xbox. http://en.wikipedia.org/wiki/Xbox, Last visited June 2007. 4.2.4

[56] Xbox 360 Technical Specifications. http://www.xbox.com/en-AU/support/xbox360/manuals/xbox360specs.htm, Last visited June 2007. 4.2.5

[57] Andrews, J. & Baker, N. 2006. Xbox 360 System Architecture. *IEEE Micro*, 26, 25–37. 4.2.5

[58] Microsoft Xbox 360 (20gb) Specs. Video Game Consoles Specifications. http://reviews.cnet.com/Microsoft_Xbox_360_20GB/4507-6464_7-31355096.html?tag=sub, Last visited June 2007. 4.2.5

[59] Wikipedia - Wii. http://en.wikipedia.org/wiki/Nintendo_wii, Last visited June 2007. 4.2.6

[60] Nintendo Wii Specs. Video Game Consoles Specifications. http://reviews.cnet.com/Nintendo_Wii/4507-6464_7-31355104.html?tag=sub, Last visited June 2007. 4.2.6

[61] Wii Specifications. http://www.wii-volution.com/wii-specifications.html, Last visited June 2007. 4.2.6

[62] Wii - WiiConnect24. http://www.nintendo.com/consumer/systems/wii/en_na/settingsWiiConnect24.jsp, Last visited June 2007. 4.2.6

[63] Complete Nintendo DS technical specs. http://www.nintendo.com/techspecds, Last visited June 2007. 4.2.7, 5.9

[64] Nintendo DS Lite (polar white) Specs. Consoles Specifications. http://reviews.cnet.com/Nintendo_DS_Lite_polar_white/4507-10109_7-31756952.html?tag=sub, Last visited June 2007. 4.2.7

[65] Nmap. http://insecure.org/nmap/, Last visited June 2007. 4.3.1

[66] Nessus. http://www.nessus.org/, Last visited June 2007. 4.3.2

[67] The Metasploit Project. http://www.metasploit.com/, Last visited June 2007. 4.3.4

[68] SPSS Homepage. http://www.spss.com/, Last visited June 2007. 4.3.5

[69] National Vulnerability Database (CVE-2004-0268). http://nvd.nist.gov/nvd.cfm?cvename=CVE-2004-0268, Last visited June 2007. 5.2.1

[70] Membership Levels - Gold and Silver. http://www.xbox.com/en-US/live/memberships/?WT.svl=nav, Last visited June 2007. 5.5

[71] Internet Assigned Numbers Authority. http://www.iana.org/, Last visited June 2007. 5.5, 5.8.2

[72] Isensee, P. Xbox Secure Sockets. 5.5.1, 5.5.2

[73] The Keyed-Hash Message Authentication Code. http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf, Last visited June 2007. 5.5.2

[74] Isensee, P. Xbox Security Architecture. 5.5.2

[75] PS2 Network Adaptor FAQ. http://boardsus.playstation.com/playstation/NetworkAdaptorFAQ, Last visited June 2007. 5.6

[76] National Vulnerability Database (CVE-2005-2577). http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-2577, Last visited June 2007. 5.8.1

[77] Get to Know the Web on Wii: Full Version of Wii Internet Channel Powered by Opera Available for Free Download. http://www.opera.com/pressreleases/en/2007/04/12/, Last visited June 2007. 5.8.2

[78] The TLS Protocol Version 1.0. http://tools.ietf.org/html/rfc2246, Last visited June 2007. 5.8.2

[79] Nintendo Wii Firewall / Antivirus / Antispyware / Adware Compatibility Info. http://wiiportal.nintendo-europe.com/75.html, Last visited June 2007. 5.8.2

[80] Akamai Leveraged as Content Delivery Infrastructure for Nintendo Wii. http://www.akamai.com/html/about/press/releases/2006/press_121906b.html, Last visited June 2007. 5.8.3

[81] Violent Video Games - Psychologists help Protect Children from Harmful Effects. http://www.psychologymatters.org/videogames.html, Last visited June 2007. 6.4

[82] Entertainment Software Association. Top 10 Industry Facts. http://www.theesa.com/facts/top_10_facts.php, Last visited June 2007. 6.4

[83] Entertainment Software Rating Board Homepage. http://www.esrb.org/, Last visited June 2007. 6.10

[84] Pan European Game Information Homepage. http://www.pegi.info/, Last visited June 2007. 6.10

[85] Battle.net emulator broke DMCA and EULA. http://www.out-law.com/page-6087, Last visited June 2007. 8.1

[86] Gjerde, R. Browser eavesdropping - how can we prevent our browsers from revealing our private information. Master's thesis, Gjøvik University College, 2005. 8.1

[87] Wii, cellphone net surfers face attack risk. http://www.cbc.ca/technology/story/2007/04/23/tech-operawiicellphonerisk-20070423.html, Last visited June 2007. 8.1

9 Appendices

9.1 The questionnaire (Norwegian)

Høgskolen i Gjøvik i samarbeid med Gjøvik kommune og Skolekontoret

Høgskolen i Gjøvik avdeling for Informatikk og medieteknikk

Fredag 27. april 2007

Til foresatte

Som del av en masteroppgave ved Høgskolen i Gjøvik så ønsker vi å gjennomføre en spørreundersøkelse blant foreldre med barn i grunnskolen. Vi ønsker å få ett klarere bilde av foreldres oppfatning av hvordan barn bruker Internett, og hva foreldre vet om barnas bruk av Internett. Samtidig så ønsker vi også å undersøke hvordan foreldre forholder seg til barns bruk av data og tvspill på Internett, og hvordan foreldre tror barn oppfører seg i virtuelle verdener. Dette gjelder spesielt hvordan barn behandler sine egne personopplysninger* når de bruker Internett.

Spørreundersøkelsen gjennomføres i samarbeid Gjøvik kommune og skolekontoret og resultatene av undersøkelsen vil bli gjort tilgjengelig for kommunen slik at de kan brukes til å bedre skolenes undervisningstilbud til barn og unge. De vil også bli publisert som del av den ferdige masteroppgaven.

All informasjon som blir samlet inn blir anonymisert og vil bli behandlet konfidensielt. Vi setter meget stor pris på om du kan sette av 10 minutter av dine travle hverdag til å svare på spørsmålene og legge dem i vedlagt konvolutt. Konvoluttene skal taes med tilbake til skolen slik at de kan bli samlet inn. Vi takker på forhånd for deltagelsen.

Med vennlig hilsen

Halvar Myrmo
Master i informasjonssikkerhet

Ord og uttrykk market med en * har en kort forklaring på siste side.

Vennligst svar ja, nei eller vet ikke på følgende spørsmål:

	Ja	Nei	Vet ikke
1. Det finnes datamaskin i hjemmet som barnet(ene) har tilgang til å bruke	□	□	□
2. Barnet(ene) har tilgang til Internett hjemme	□	□	□
3. Vi har spillkonsoll(er) som er koblet til Internett	□	□	□
4. Vi bruker brannmur på datamaskinen	□	□	□
5. Vi bruker antivirus på datamaskinen	□	□	□

På en skala fra 1 til 5, hvor 1 er helt enig og 5 er helt uenig, hvordan stiller du deg til følgende utsagn:

	Helt enig				Helt uenig	Vet ikke
6. Jeg har opplevd at datamaskinen har blitt infisert av virus eller lignende	○	○	○	○	○	□
7. Bruk av passord er en smart måte å sikre informasjon på	○	○	○	○	○	□
8. Jeg syntes det er for mange tjenester som bruker passord på Internett	○	○	○	○	○	□
9. Jeg har skrevet ned passord fordi det blir for mange å huske på	○	○	○	○	○	□
10. Jeg bruker det samme passordet til flere tjenester	○	○	○	○	○	□
11. Barn burde ha mulighet for å bruke Internett uten overoppsyn fra voksne	○	○	○	○	○	□
12. Jeg mener det er viktig for skolegangen at barn behersker bruk av datamaskin og Internett	○	○	○	○	○	□
13. Loggene* etter barnets(enes) bruk av Internett bør gjennomgåes for å ha en oversikt over hva de har drevet med	○	○	○	○	○	□
14. Loggene etter barnets(enes) bruk av Internett bør gjennomgåes for å ha en oversikt over hva de har drevet med, uten at de er klar over det	○	○	○	○	○	□
15. Nettvett* er ett tema som har blitt tatt opp med barnet(ene) hjemme	○	○	○	○	○	□
16. Nettvett er ett tema som barnet(ene) lærer på skolen	○	○	○	○	○	□
17. Nettvett er ett tema som har blitt tatt opp i forhold til spillverdener og virtuelle verdener på Internett	○	○	○	○	○	□
18. Barnet(ene) har lagt ut bilder av seg selv på Internett	○	○	○	○	○	□
19. Hvis barnet(ene) spurte om lov til å legge ut bilder av seg selv på Internett så ville de fått lov	○	○	○	○	○	□
20. Barnet(ene) har lagt ut personopplysninger* om seg selv på Internett som jeg ønsker de ikke hadde lagt ut	○	○	○	○	○	□
21. Barnet(ene) har møtt noen de har hatt kontakt med på Internett i det virkelige liv	○	○	○	○	○	□
22. Barnet(ene) har møtt noen de spiller sammen med på Internett i det virkelige liv	○	○	○	○	○	□
23. Jeg mener spilling av data/tvspill på Internett er usosialt	○	○	○	○	○	□
24. Jeg mener at det er lurt å begrense barns tidsbruk når det gjelder spilling av data/ tvspill	○	○	○	○	○	□
25. Min oppfattning er at barn kan bli voldelige av å spille data/tvspill som inneholder vold	○	○	○	○	○	□
26. Jeg mener barn heller burde drive med sport enn å spille data/tvspill	○	○	○	○	○	□
27. Jeg mener barn blir passive av å spille data/tvspill	○	○	○	○	○	□
28. Det er lurt av voksne å spille data/tvspill sammen med barna, slik at de får innsikt i barns bruk av dette mediet	○	○	○	○	○	□
29. Det er tryggere at barnet(ene) spiller på en spillkonsoll enn at de surfer på Internett	○	○	○	○	○	□
30. Spillkonsoller som er koblet til Internett er ett mål for virus	○	○	○	○	○	□
31. Vi bruker mulighetene i spillkonsollene til å styre hva slags innhold barnet(ene) har tilgang til	○	○	○	○	○	□

Hva slags spillkonsoller har dere? Flere valg mulig:

Xbox □

Xbox 360 □

PlayStation 2 □

PlayStation 3 □

PlayStation Portable □

Nintendo GameCube □

Nintendo Wii □

Nintendo GameBoy □

Nintendo DS □

Bruker datamaskin til spilling □

Ingen av delene □

Annet: ______________________________

Generelle opplysninger

Hvem fyller ut undersøkelsen: ○ Mor ○ Far ○ Andre

Vennligst fyll inn klassetrinn og kjønn for barnet(ene)

	Klassetrinn	Kjønn
Barn 1:	□	○ Gutt ○ Jente
Barn 2:	□	○ Gutt ○ Jente
Barn 3:	□	○ Gutt ○ Jente

Utdanningsnivå foreldre:

Jeg: ○ Ungdomsskole ○ Videregående skole ○ Høgskole/Universitet

Partner: ○ Ungdomsskole ○ Videregående skole ○ Høgskole/Universitet

Foreldres bruk av datamaskin og Internett:

Jeg:

□ Bruker datamaskin på jobb

□ Bruker Internett på jobb

□ Bruker datamaskin hjemme

□ Bruker Internett hjemme

□ Bruker e-post

□ Chatter (Messenger, IRC, ICQ)

□ Spiller dataspill/tvspill

Partner:

□ Bruker datamaskin på jobb

□ Bruker Internett på jobb

□ Bruker datamaskin hjemme

□ Bruker Internett hjemme

□ Bruker e-post

□ Chatter (Messenger, IRC, ICQ)

□ Spiller dataspill/tvspill

Personopplysning

Personopplysning er en opplysning som kan knyttes til en enkelt person. Det betyr at for eksempel navn, alder, adresse og telefonnummer er personopplysninger dersom de kan knyttes kun til deg. Hvis du bare skriver alderen din på nettet er det derfor ikke en personopplysning siden det er mange som har samme alder. Men; dersom du samtidig skriver adressen din og kanskje også navnet ditt vil det likevel bli en personopplysning siden det som regel er få med samme navn og alder på en bestemt adresse. Bilder der du kan kjennes igjen er også en personopplysning.

Nettvett

Nettvett er Internettets form for trafikkregler. Det er regler som er ment å skulle gi barn ett rammeverk for hvordan man kan bruke Internett fornuftig. På samme måte som voksne i alle år har lært barna sine å se seg for når de skal krysse gaten, eller aldri sette seg i bilen til en fremmed så må de læres opp til å bruke Internett på en fornuftig måte.

Logg

Alle programmer som brukes på Internett legger igjen spor etter seg. Disse sporene finnes også på den datamaskinen som brukes, og det er derfor mulig å få oversikt over hva andre har brukt maskinen til. Det kan være veldig mye informasjon som loggføres uten at den som bruker Internett er klar over det, og dette kan føre til at det er mulig å overvåke noens Internettbruk uten at de er klar over det.

Definisjonene er hentet fra Statens filmtilsyn, BarneVakten og Saft sine hjemmesider.

9.2 The questionnaire (English translation)

Some of the expressions and language used are not directly translatable to English. Therefore there might be some slight inconsistencies between the Norwegian questionnaire and the English translation, but the essence should be the same.

Gjøvik University College in cooperation with Gjøvik municipality and Skolekontoret

Gjøvik University College department of Informatics and media technique

Friday 27 of April 2007

To the parents

As part of my master thesis at Gjøvik University College we wish to conduct a survey among parents with children in grade school. We wish to map parents apprehension of how children use Internet and what parents know about their children's use of Internet. At the same time we wish to look into how parents relate to children's use of computer and video games on the Internet and how parents think that children behave in virtual worlds. This is specifically targeted towards how children treat their own personal information* when using the Internet.

The survey is conducted in cooperation with Gjøvik municipality and the office for schools, and the results will be made available for the municipality so that it can be used to improve the educational conditions of the schools. They will also be published as part of the finished master thesis.

All information that is gathered will be anonymous and treated with confidentiality. We will greatly appreciate if you can set aside 10 minutes of your daily schedule to answer the questions, and then but it back in the envelope. The envelopes should be taken back to the school, were they will be collected. We thank you in advance for participating.

Regards

Halvar Myrmo
Master in information security

Words and expressions marked with a * has a short explanation at the last page.

Please answer yes, no, or don't know on the following questions:

	Yes	No	Don't know
1. There are computers in the home that the child(ren) has access to	□	□	□
2. The child(ren) has access to the Internet at home	□	□	□
3. We have game consoles that are connected to the Internet	□	□	□
4. We use a firewall on our computer	□	□	□
5. We use antivirus on our computer	□	□	□

On a scale from 1 to 5, were 1 is agree and 5 is disagree, what do you think of the following statements:

	Agree				Disagree	Don't know
6. I have experienced that my computer has been infected with a virus or similar	○	○	○	○	○	□
7. The usage of passwords is a smart way to protect information	○	○	○	○	○	□
8. I feel there are too many services that use passwords on the Internet	○	○	○	○	○	□
9. I have written down passwords because there are too many to remember	○	○	○	○	○	□
10. I use the same password for several services	○	○	○	○	○	□
11. Children should have the possibility of using the Internet without adult supervision	○	○	○	○	○	□
12. I feel that it is important in for the education that children can use computers and the Internet	○	○	○	○	○	□
13. The data logs* of children's Internet usage should be checked to get an overview of what they are doing	○	○	○	○	○	□
14. The data logs of children's Internet usage should be checked to get an overview of what they are doing, without them knowing of it	○	○	○	○	○	□
15. Netiquette* is a subject that has been discussed with the child(ren) at home	○	○	○	○	○	□
16. Netiquette is a subject that the child(ren) learn in school	○	○	○	○	○	□
17. Netiquette is a subject that has been discussed in regards to game worlds and virtual worlds on the Internet	○	○	○	○	○	□
18. The child(ren) has posted images of themselves on the Internet	○	○	○	○	○	□
19. If the child(ren) asked for permission to post images of them selves on the Internet, they would be allowed to do so	○	○	○	○	○	□
20. The child(ren) har posted personal information* about themselves on the Internet that I wish they hadn't	○	○	○	○	○	□
21. The child(ren) has met someone they have contact with over the Internet, in real life	○	○	○	○	○	□
22. The child(ren) has met someone they play on the Internet with, in real life	○	○	○	○	○	□
23. I feel that playing computer/video games on the Internet is unsocial	○	○	○	○	○	□
24. I feel that it is smart to limit children's time usage when it comes to playing computer and video games	○	○	○	○	○	□
25. I think children can become violent by playing computer/video games that contains violence	○	○	○	○	○	□
26. I feel that children rather should be doing sports than playing computer/video games	○	○	○	○	○	□
27. I think children become inactive by playing computer/video games	○	○	○	○	○	□
28. It is smart of adults to play computer/video games with the children, in order to get knowledge of children's use of this medium	○	○	○	○	○	□
29. It is safer for the child(ren) to play on a game console than surfing on the Internet	○	○	○	○	○	□
30. Game consoles that are connected to the Internet are a target for virus	○	○	○	○	○	□
31. We use the built-in possibilities in the game consoles to control what kind of contents the child(ren) has access to.	○	○	○	○	○	□

What kind of game consoles do you have? Multiple choices possible:

Xbox □
Xbox 360 □
PlayStation 2 □
PlayStation 3 □
PlayStation Portable □
Nintendo GameCube □
Nintendo Wii □
Nintendo GameBoy □
Nintendo DS □
We use the computer for gaming □
Neither □

Other: ______________________________

General information

Who is filling out the questionnaire: ○ Mother ○ Father ○ Someone else

Please fill in grade and gender of the child(ren):

	Grade	Gender
Child 1:	□	○ Boy ○ Girl
Child 2:	□	○ Boy ○ Girl
Child 3:	□	○ Boy ○ Girl

Parents education:

Me: ○ Junior high school ○ College ○ University college /University
Partner: ○ Junior high school ○ College ○ University college /University

Parents usage of computers and Internet:

Me:

□ Uses computer at work
□ Uses Internet at work
□ Uses computer at home
□ Uses Internet at home
□ Uses e-mail
□ Uses online chat
□ Plays computer/video games

Partner:

□ Uses computer at work
□ Uses Internet at work
□ Uses computer at home
□ Uses Internet at home
□ Uses e-mail
□ Uses online chat
□ Plays computer/video games

Personal information

Personal information is information that can be tied to a single person. This means that for example name, age, address and phone number are personal information if they can be tied to only you. If you only write your age on the Internet it is not considered personal information since there are many with the same age. But if you at the same time write your address and maybe your name also, it becomes personal information since there rarely are persons with the same name and age living at the same address. Images where you can be recognised is also personal information.

Netiquette

Netiquette is the traffic rules of the Internet. They are rules meant to give children a framework for how to use the Internet in a reasonable way. The same way that grown ups has taught children for years to look before crossing a street, or never get into a car with a stranger, so they must also be taught how to use the Internet in reasonable ways.

Data log

All programs that are used on the Internet leaves traces behind. These traces also exist on the computer on which the program is run, and make it possible to get a good overview of what other uses the computer for. A lot of information can be logged this way without the knowledge of the user, and this might lead to possible surveillance of someone's use of the Internet without them knowing.

The definitions are gathered from the homepages of Statens filmtilsyn, BarneVakten and Saft.