Social Gaming in a Privacy and Integrity Context

Fredrik Westmark

October 2, 2006
Master's Thesis in Computing Science, 20 credits
Supervisor at CS-UmU: Anders Broberg
Examiner: Per Lindström

Umeå University
Department of Computing Science
SE-901 87 UMEÅ
SWEDEN

Abstract

Recent advances in technology have brought us world turning applications, such as the Internet. Something that was unheard of only a few decades ago, nameley electronic surveillance in all its forms, has become almost commonplace. In turn, we have a novel problem at our hands, that of privacy and integrity in a networked world. This paper aims to offer a definition to the elusive term "privacy", explain some of the threats against it, and to report on the general opinion regarding these threats.

When working together towards a common goal, people may sometimes behave differently from their everyday lifes. Some will even deliberately make fools of themselves, all for the sake of the group. For the purpose of studying this behavior, an application which works with audio-visual input, among others, has been implemented. This application takes the form of a game console with loadable games. Input comes in the form of sensory data collected from any imaginable source that can in some way produce a representation of its immediate surroundings. Obvious examples are cameras and microphones. Combined together, this data can be used to control an in-game avatar.

For the purpose of demonstrating this application, as well as to conduct rudimentary experiments concerning social gaming, a Ping-Pong clone has been implemented.

Contents

1 Introduction **1**

1.1 What is Peer-to-Peer 1

1.1.1 Different Kinds of Peer-to-Peer Networks 2

1.2 Social Interaction 2

1.3 Problem Specification 3

1.4 Method 3

1.5 Structure of the report 5

2 Privacy and Personal Integrity **7**

2.1 Defining "Privacy" 7

2.1.1 Common Concerns 8

2.1.2 Altman's Privacy Theory 8

2.1.3 Palen and Dourish's Privacy Theory 8

2.2 Privacy Issues Today 10

2.2.1 Privacy Issues Mediated by the Internet 10

2.2.2 Information Gathering Through Customer Cards 12

2.2.3 Positioning 13

2.2.4 Surveillance 13

2.3 Attitudes about Privacy 14

2.3.1 Online privacy 14

2.3.2 Everyday Privacy 17

2.4 Conclusions 18

3 Implementation **21**

3.1 General overview 21

3.2 Sub-system Details 22

3.2.1 The Sensor 22

3.2.2 Vastus Engine 25

3.3 Ping-Pong 26

4 Conclusion **27**

5 Future Work **29**

6 Acknowledgements **31**

References **33**

A Vastus Usage **35**

B How to Write a Game for Vastus **39**

Chapter 1

Introduction

Social interaction is a hot subject within modern computing scientific research. The advent of the Internet has made it possible for users spread out all over the world to come together in *communities*, and also to study how these interact. Social psychology researchers can for the first time in history observe how literally millions of users gather together, in the same place, and at the same time. For them a whole new area of research has suddenly opened up. Tools that facilitate the creation of the so called communities, e.g. Wiki[22] and phpBB[19], have been around on a smaller scale for some time, but it is not until very recently that these have evolved into the (somewhat) user-friendly and powerful tools that they are today. One of foundations for these tools is the so called *peer-to-peer*-architecture.

1.1 What is Peer-to-Peer

The term peer-to-peer, or *P2P*, was relatively unknown until just a few years back, being used as it was, by no one save the most prominent minds within the field of network technology. Since then hundreds, if not thousands, of applications built on P2P-technology have seen the light of day, with many of them being among the most used application today. Among them Napster [14], KaZaA [13], and Gnutella [9] are all widely known and used so called *file sharing applications*, which to a varying degree are based on the P2P-arcitechture. Several other file sharing applications use the BitTorrernt [5] protocol, which is a quite elaborate file sharing scheme that emerged a few years back. One should note however, that peer-to-peer is more than just file sharing even if that seems to be the opinion of the masses. Projects like Seti@Home [20], OceanStore [16], and Genome@Home [8] are more about *resource sharing*, e.g. CPU-cycles, storage space, etc., than file sharing.

Why then should you employ the peer-to-peer architecture? What are the advantages comepared to the classic concept of a centralized server or even a server cluster? A *perfect* P2P-network has no dedicated servers at all; all nodes, i.e. clients, in the network are completely equal in terms of function. In fact, each node functions both as a client and a server at the same time. This effectively produces a highly stable network topology, where the failure of one node will have little or no effect on the rest of the network, unless of course the network is very very small. When a node goes down, the network should be able to retain stability without the assistance of a human administrator, which is needed for a network with one or several centralized servers. Since there is no single node that

has to maintain exactly all client connections, a P2P-network scales much better than its centralized counter-part. Administration and responsibility for the maintenance of a P2P-network falls on the users themselves. A network where the users have all the power will, for obvious reasons, be more resistant to censorship[3]

In this report the terms peer-to-peer and P2P will be used interchangeably.

1.1.1 Different Kinds of Peer-to-Peer Networks

As stated before, a perfect P2P-network is said to be a network of interconnected nodes where all nodes are completely equal in function. The common approach is however to keep some kind of centralized server which serves non-critical funtions such as reputation and grading services. Some networks, KaZaA for instance, rely on the use of supernodes. A supernode is essentially a client node that has accepted to function as a kind of mini server which is used to facilitate functions such as indexing. These network types are usually regarded as P2P-networks, even if they do not fully follow the above definition of a perfect P2P-network[3].

With such a strict definition, it is difficult to see how applications such as Seti@Home fits into the P2P category. Seti@Home is essentially an elaborate calculator which performs calculations on small packets of radio transmission data collected at some radio observatory somewhere on the globe. The client depends on a centralized server from which it receives these data packets. If the server is down, the client can do nothing. Neither is there any data passed between the clients themselves. To that end, Shirky[21] gives us this definition of peer-to-peer; "peer-to-peer is a class of applications that take advantage of resources - storage, cycles, content, human presence - available at the edges of the internet". What Shirky is trying to say is that a whether a network can be regarded as P2P compliant should not be exclusively decided by its technical aspects such as stability and scalability, but rather also by the *services* the network can provide. Needless to say, there are many different views on how P2P should be defined.

1.2 Social Interaction

The human animal is a flock animal, and if she has the opportunity to socialize with like minded individuals she will often do it. However, in order to socialize, physical proximity is not always necessary. The positive feeling of belonging, even if physically at a distance, can go very far. This sensation is further reinforced when participating in whatever project is being worked on by the group. Peter Kropotkin, a russian prince, geographer and outspoken anarchist who lived in the end of the nineteenth centurty, disliked Darwin's theories on competition being the first and foremost driving force behind evolution. Kroptokin instead argued that *cooperation* had to be a more potent factor in the history of human success[11]. Whether Kropotkin was right is beyond the scope of this thesis, but the fact remains; to cooperate with our peers and to see the efforts bear fruit is usually regarded as a favourable prospect by us humans. This may be, and most likely is, one of the main reasons why the Internet has become some successful since the day of its commercialization. The Internet brought with it the tools for interacting and cooperating with known or even unknown people from all over the world, regardless of actual physical distance. Those involved could communicate more or less instantly with each other thanks to e-mail, IRC, ICQ and other chat related protocols. The modern Internet is a veritable treasure trove full of examples on how much we love to create together, the Open Source-scene being perhaps the most prominent example. So called

Wiki-pages[22], where anyone can change or add to the content, are cropping up like mushrooms and inviting people to share their knowledge, expertise, and experiences. Online games such as Everquest, Dark Age of Camelot, Star Wars: Galaxies, and last but not least the immensely popular World of Warcraft allow literally millions of players to gather and populate a fictive world that only exists in the so called cyberspace, in the participants' collective imagination.

1.3 Problem Specification

Needless to say, people in general behave very differently when on their own compared to being in a group. Add some kind of activity where winning and losing, possibly against another group, is involved and that behaviour changes even more. To realize this, one only has to look to the millions of soccer fans totally losing it, in a positive or negative way, when the home team wins or loses the game. Some people are willing to make complete fools of themselves just for the sake of the group. The purpose of this thesis is to create a platform where this so called *silly* behaviour can be encouraged and subsequently studied. The platform itself will be a game console with a distributed interface, meaning that the input to the console consists of data from several *sensors*. A sensor can be just about anything that can monitor its surrounding environment, transform this information into data packets and subseqently send/stream these to the console, or even consoles. Examples of sensors includes cameras, microphones, touch pads, motion detectors, and so on. Each sensor keeps a list of *subscribers* and streams its data to each of them at a rate set by the subscriber. From now on the terms *subscriber* and *node* will be used interchangeably. The node is responsible for initiating the connection with the sensor. After receiving a chunk of data, the node will perform some calculation on it, use the result to affect the game world, and the make the transformed chunk available to other nodes in the network. These nodes will process the chunk once again, use it, make it available to others, and so it goes on. This way input can be shared by all nodes in the network. The sensors are the only components that do not subscribe to any information.

Figure 1.1 displays an example network. Notice how each node, except the bottom one, functions as both server and client. This configuration assumes the form of a P2P-network, as all nodes are roughly identical in function with some nodes (the sensors) having special assignments, and information is exchanged in all directions.

For the sake of simplicity, a thin client which will receive game data from the console and display it for the user, as well as one game; Ping-Pong, will also be implemented. The thin client will only act as a pure client, and will thus not forward data to any other node. It is assumed that the thin client knows which game is currently played, and how to interpret incoming data.

1.4 Method

As information technology becomes an increasingly large part of our daily lives, a very important detail must continously be provided for, and that is the notion of personal privacy, or personal integrity. George Orwell, with his book *1984*, may well have been the instigator of the debate regarding "big brother" and the potential dangers to personal integrity. In today's electronically ridden society it is nearly impossible to *not* leave a trail of virtual breadcrumbs after youself in your everyday life. Surveillance cameras

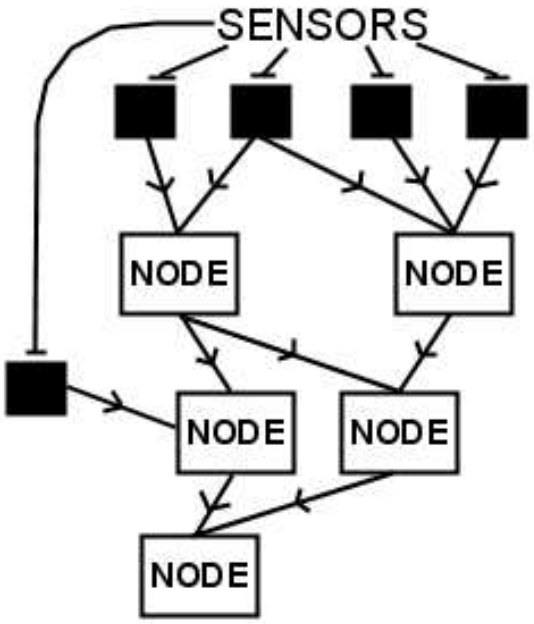

Figure 1.1: Example network

are present in most shopping malls, supermarkets, road intersections, and other public places, even in taxi cars. Credit card transactions will reveal your position at a certain point in time, and also what you bought and how much money you spent on it. RFID (Radio Frequency Identification) tags are being incorporated into a daily increasing number of products, our cell phones can easily be positioned without any special equipment, and the same goes for laptops with WLAN (Wireless Local Area Network)-connection. Each time we visit a homepage or use an application that communicates via the Internet we risk our activites being noted and recorded. Whatever trace we leave behind can be processed in a multitude of ways, that stretches from pure concern to pure interest in profit, possibly even registration of political opinions. Applications based on P2P can be very vulnerable from an integrity standpoint, since the usage of the application often means that we surrender some information about ourselves[7][4].

So, is this an acceptable situation? Research has shown that there are many aspects that factor in when we decide if we should feel violated or not[4], but how can we determine if we are? Is it a gut feeling, or is there perhaps a set of rules that can help us? Cameras and such are very tangible ways of surveillance, but there are other tools that act mostly unseen. What are they, and how do they work? And what exactly does the word "privacy" entail? If privacy can be defined, is it also possible to determine if it is at all affected by modern technology? These are all questions that require an answer. The purpose of this report is perhaps not to give all of those answers, but to explain the current situation, and to serve as a basis for discussion.

1.5 Structure of the report

This paper is divided into two main parts. The first part deals with privacy and personal integrity. It begins by offering a definition to the notion of privacy, and moves on to present a variety of privacy threats that exist today. These threats are briefly discussed in light of the previous definition of privacy.

The second part covers the implementation specifics of the Vastus game engine. Manual and a short tutorial on writing games for Vastus are attached as appendices.

Chapter 2

Privacy and Personal Integrity

> –"*Any society that would give up a little liberty to gain a little security will deserve neither and lose both*"
>
> Benjamin Franklin

We are living in the golden childhood age of information technology, and it is not without teething problems. In a world getting more interconnected for each day that passes it may not be surprising that the debate concerning privacy and personal integrity suddenly is of immediate interest. We are also living in a world where the competition between the corporations to reach us, the consumers, is stiffer than ever. Suddenly there are incentives for a market player to analyze what, how, and when we consume, watch on TV, which sport activites we are engaged in, and so on, all for the sake of offering us tailored offerings and thus make us prefer that specific supplier. Of course this behaviour is not always condoned by the consumers as they feel their personal integrity has been violated. But what is privacy, or its close relaive; integrity? In order to protect our privacy, we must first know what it is. The notion itself is immensely hard to define due to a number of reasons as we shall see. These obstacles must however not stop us from dealing with the problem at hand. The author and debater Anders S. Olsson writes "Even though the term 'personal integrity' is nuanced, ideologically controversial and at times technologically complicated, it must not push us towards passiveness"[2].

2.1 Defining "Privacy"

Privacy as a notion is extremely hard to define. According to Peter Siepel, there are three main causes for this. 1) It concerns an individuals personal and subjective view upon discomfort and powerlessness. 2) The legislation should work as a skeleton law, but at the same time specific cases require alternative interpretations. 3) What is regarded as intrusion into our personal lives is determined by the attitudes and political values of different action groups[18].

Despite broad concern about the subject of privacy there have been few analytic or systematic attempts to help us better understand the relationship between privacy and technology. Even though we might recognize the "privacy issues" introduced by our systems, we have few tools for understanding exactly what these issues are. In an effort to device such tools, Palen and Dourish[17] introduced the notion of *privacy*

boundaries which will be presented here. Their work is based on the privacy theories of Irwin Altman[12][1], who began his work on privacy theory in the 1970s.

2.1.1 Common Concerns

Concerns about surveillance and personal identity theft are ususally heavily discussed when privacy is debated. These may be important issues as they may very well constitue a law breach, but research has shown that users are significantly more concerned about minimizing embarrassment, protecting turf, and staying in control of ones own time. To put it another way, users tend to emphasize more on issues that concern vanity. Although the former mentioned so called "Big Brother" actions very well could threaten life and liberty, it is interpersonal privacy matters that dictates our decisions about technology use on an everyday basis[17].

Back in the days when electricity was just a fairy tale, we relied on the inaudability of conversations at a distance, and our inability to see through walls to manage our personal privacy. That is no longer the case, since technological advances have changed and in some cases even obliterated the possibilities of using spatial and physical features to keep our conversations hidden. In a virtual setting, our audience can not be explicitly chosen; it chooses us. In addition, the recordability and subsequent persistance of information, especially that which was once ephemeral, means that audiences may not only exist at the time of disclosure, they will exist in the future as well[17].

2.1.2 Altman's Privacy Theory

The traditional approach to defining privacy is to describe it as a state of withdrawal. This definition is sketchy at best, as privacy is not monotonic, meaning that more privacy is not necessarily better. In fact, both total withdrawal, or isolation, and total "crowding" are the result of privacy regulation gone wrong. Altman does not believe in rule-based or static privacy regulation. As such, privacy must be regarded as something that is relative to what is desired, and to what is actually achieved. That is to say, even in the presence of others one might feel isolated depending on the degree of sociability sought. According to Altman, privacy can be conceptualized as the "selective control of access to the self" regulated as dialectic and dynamic processess. Privacy is, according to Altman, a *boundary regulation process*. This process is described as, depending on context, fine-tuning your own accessabilty along a spectrum of "closedness" and "openness".

There are limitations to Altman's theories, as they address only the personal access in public spaces and other forms of interpersonal interactions. In other words, Altman's theories are devoted to situations which take place in the everyday spatial environment. To incorporate these theories into the networked world, Palen and Dourish have built upon Altman's theories to establish the concept of *circumstance*, which they define to be a function of the local physical environment, audience, social status, task or objective, motivation and intention, and finally, information technologies in use.

2.1.3 Palen and Dourish's Privacy Theory

Palen and Dourish base their privacy theories around three *boundaries*. These boundaries divide conflicting goals, and represent the tensions between them. Privacy management is defined as the process of regulating the degree of disclosure between these goals. When context changes, so do the boundaries. Information technology factors into

this view by its ability to disrupt and destabilize the regulation of boundaries. It can mediate transformations in the boundaries, be a means of managing boundaries, and so forth. The three boundaries that Palen and Dourish believe are central to the definition of privacy management, are

- the *Disclosure* boundary, where privacy and publicity and in tension,
- the *Identity* boundary, where the self and other are in tensions, and finally,
- the *Temporality* boundary where the past, present and future are in tension.

All three boundaries are not to be seen as separate, but rather quite interconnected as they often affect each other.

The disclosure boundary aims to rid us of the notion that privacy regulation in practice is not simply a matter of avoiding information disclosure. In order to function in any society, one must be ready to disclose personal information about oneself, although selectively. In fact, most people go to great lengths in order to promote themselves this way or the other, and in the process of doing so publicize their opinions and activities as a means of declaring allegiance or even of differentiating themselves from others. Managing privacy means paying attention to both one's personal live and one's public face. To function in a modern society, or in order to safeguard one's saftey somewhat, disclosure may even be *required*. Some people choose not to take the shortcut through that dark alley, but instead walks down the public street; saftey by living publicly. Another example that involves the networked world is when we buy goods online. In this case we choose to disclose personal information and possibly credit card numbers, and in doing so we assume some risk of identity theft. The problems become obvious when participation in the networked world is not deliberate. Using a search engine, one can find out a lot of information about a person, even goings and doings in the past which may or may not be consistent with one's self-perception today. As these examples show, the tension around privacy and publicity is also influenced by identity and temporal concerns, which are addressed in turn.

The second boundary, the identity boundary, is concerned with the tension between the "self" and the "other". Palen and Dourush refer to a phenomenon they call *recipient design*, in which one's actions and utterances are largely designed with respect to specific others. In other words, as well as the "self" may take on different faces given a set of social arrangements, so will also our view on the "others". Depending on the recipient, our treatment of him/her will be different depending on our relationship. It is fair to say that close professional colleagues are treated very differently from total strangers on the bus. The tension can be clarified by the problem with surveillance cameras in public places. The usual argument is that your actions in a public place is "already public", so why should you bother with being caught on tape? This argument, however, fails to recognize how broadly faceted the concept of "public" really is. To deny the ability to rn who might be able to see one's actions can, in itself, constiture a violation of personal privacy. Another complication concerned with the regulation of the self/non-self boundary is that of information persistance. Old products of work or activity, such as manuscripts posted on a web page, forum and mailing list postings, and so on, can be used to construct and control how we will be perceived by others. This problem is further enhanced by our inability to control representations of ourselves that are artifacts of simply having been somewhere or done something at a particular time. Recipients vary greatly in ideologies and opinions, which has a direct impact on how

we are perceived. Over time, interpretations may change, and once again we see how a little control the person whom the information represents actually has.

The general idea behind the temporal boundary is that specific instances of information disclosure are not necessarily separate, but rather occur as a sequence of historical actions, and will form the basis for future actions. Current actions are seen and dissected by our audience in the light of our past presentations, meaning that the reactions and responses that will be received in the future are will likely be similar to those received in the past. This argument is of course highly connected to the self/non-self boundary. Also introduced by the temporal boundary is the temporal nature of disclosure, which is affected by the ability of modern technologty to easily distribute information and last but not least, *make ephemeral information persistent*. Privacy regulation is not necessarily hindered by this; it is rather a part of the ongoing management of tensions, in which information permanence becomes just as important notion as impermanence. They both affect regulatory behaviour in ways of constraining, undermining, and modifying it. The only way to gain some control is to use a format of information that cannot easily be altered, such as using cryptographic signatures or PDF to distribute content instead of Microsoft Word files, which can easily be modified by anyone having the correct software installed.

These are the three boundaries which demonstate that privacy regulation is a dynamic, dialectic, and negotiated affair. Palen and Dourish hold true that personal privacy is not directly supported or interfered with by technology, which rather has a destabilizing effect on the delicate and complex web of regulatory practices[17].

2.2 Privacy Issues Today

Privacy issues come in many flavours. Some are simple in nature and are easily defined and noted, while others are less tangible. In whatever form they present themselves, one must be aware in what way, if any, they may threaten our personal privacy.

2.2.1 Privacy Issues Mediated by the Internet

The Internet is the latest and probably the fastest expanding medium in which our personal privacy may be at risk if not regulated properly. Simply by starting up your favourite web browser you run the risk of having your actions recorded and stored in some database on some server which location you are totally unaware of. A worldwide spanning net of data is created as these databases are combined. Granted, there are laws in certain countries prohibiting cross-database correlations, but who can make sure that those laws are upheld 100%? Modern technology has enabled the creation of elaborate profiles which carefully describe the habits and lifestyle of individuals. Everytime you order goods over the Internet, visit a physician, book an airplane ticket, use a credit card, apply for a job, rent an appartment, drive your car, pay your taxes, get married, get divorced, use a smart card, request some kind of permit from the authorities, and so on, you become part of the data net. The fact that the net itself is several order of magnitudes faster and more effective than the old file cabinet full of papers only serves to complicate the problem[4].

In 1998, NetBus[23] was created Carl-Fredrik Neikter, a Swedish programmer. NetBus was one of the first widely known backdoor programs which allowed a computer running Microsoft Windows to be controlled remotely. Neikter claims he wrote NetBus to perform practical jokes on his friends, and not for illegaly breaking into computer

systems. Despite this, NetBus was extensively used for less nobler purposes than Neikter had envisioned. After NetBus, other similar programs followed and are still produced today. Even though not strictly illegal, applications like NetBus are being used extensively by employers to monitor the Internet activities of employees[15]. One can argue for and against this behaviour. Naturally, the management need to make certain that employees are doing the job they were hired to do, but scrutinizing their every move is hardly necessary and probably a waste of management time and resources. Some employees never become aware of this surveillance, but when they do it may serve as a deterrant from using company resources in an improper manner and even increase efficiency. But then again, employee morale might take a dip, not to mention that around the clock-surveillance constitutes a serious breach of personal privacy.

In a world with fierce competition, such as the world of E-commerce, catching our attention as custormers is worth its virtual weight in gold. To do that, corporations need to know more about their potential consumers. A common strategy in modern business industry is to map out target groups of potential buyers, and subsequently approach the members of those groups with individually tailored advertisments, often in the form of emails, non-anonymous mailed pamphlets or even direct telephone calls. That is to say, if your personal interests and needs are known to the corporation, they can approach you with personalized offerings. Companies such as Amazon will analyze your earlier purchases and direct you to similar products that you might find interesting. This way companies can satisfy the needs of its customer much more efficiently. However, this behaviour can have an undesireable impact on personal privacy. Overweight people, for instance, are perhaps not always so keen on being offered deals on diet pills, as this tells them somebody out of their control know they are overweight. Customer information is often gathered through the registration of user profiles. In this profile, you are encouraged to list your interests and hobbies, so that relevant advertisments can be displayed for you on your next visit. The companies argue that visitors on their site would rather see advertisments about things that interest them rather than bores them. This may bear some relevance, but there are also two arguments against profile registration. First up, the user has little or no control over the information once it has been submitted. They could be sold to a third party, and perhaps used to market products that the user has no interest in owning even though he/she fits the profile. Second, this information can be very valuable to the company, but the user rarely receives anything in return. The consumer should always question the motives of a profile gathering company, especially if they cannot provide an adequate privacy policy. Before any purchase, the consumer must always be allowed to make a well informed decision[4].

Data mining is another technique heavily employed by corporations to discover previously invisible information contained in large databases. A successful mining operation will produce new patterns and correlations in raw data. According to Covoukian, there are five kinds of informational categories that can be extracted with the use of data maning.

1. *Correlations between occasional events.* A supermarket may discover that a certain customer buys product A in 70% of all cases where product B is also bought.

2. *Correlations between events over time.* Within a given time from purchasing object A, 65% will also buy object B, and 40% will buy object C.

3. *Classification / profiling.* A company may for instance discover that customers about to abandon it exhibits a certain behaviour, in which case the company can

take action in order to retain the customer. This can be done by well-placed ads or price-cut offerings.

4. *Amassing of data*, which is used to discover connections that nobody has any knowledge of and therefore is not looking for. This technique can be used to find groups of individuals that are especially susceptible to a certain kind of commercial.

5. *Predictions*. Even though 1-4 can be used to make predictions about a certain individual's behaviour, they differ from this kind of prediction, which is of more specific nature[4].

Anders S. Olsson wrote on data mining, "If the police, taxation authoraties, or private companies can draw elaborate conclusions based on data mining and as a direct result makes certain categories of people subject for heigtened scrutiny - even if they are not criminal suspects - how abusive is that? If such scrutiny CAN be considerd abusive - is the problem then the vast databases? Or is it perhaps the norms that are the foundation for the actions taken by the authorities/companies"[2].

The Internet provides us with ample examples of when the three boundaries defined by Palen and Dourish are in tension with eachother. As shown above, the disclosure and temporal boundaries are taken to their extremes in data mining, where previously unknown information about a certain individual can be discovered, information this person probably never even knew he was submitting. How can this person regulate the use of information he or she does not even know exists? It cannot be done, unless the discoverer actually informs him or her about it. Hidden data can lie dormant for years before discovered, increasing the chance that the user forgets about the original information he or she submitted, or even changes his or hers oppionion to conflict with the "new" findings. The real problem is then of course that even though the user thinks he or she has submitted just enough personal information to gain access to that web-store, further use of that store's services may divulge more information about the user than originally intented.

2.2.2 Information Gathering Through Customer Cards

The era of customer card registration reached maturity during the 1990s. The retailers quickly realized the potential of the customer card and by the time of the millenium it was beginning to be difficult to find a larger store that didn't offer one. Customer cards are especially abundant in supermarkets and gas-stations. The customer card has two main purposes.

1. By owning a customer card that awards credits in some way, you are more likely to shop at the store to which the card belongs.

2. Purchases made by you or anyone else using your card, perhaps by a family member, will be recorded and used by the the store management send you personalized offerings based on your previous transactions.

Research has shown that very few consumers are actually aware of this process. Of course, the customer receives something in return – bonus points – for surrendering this information, but that does not negate the fact that the purpose of the customer card should be made more clear to the consumers before they register for it. Given time, the store management can determine what kind of products a customer usually buys,

which stores the frequent, their approxiamte age, sex, family situation, and what kind of dwelling they live in.

The sheer amount of information gained by companies through customer cards should prevent the self/non-self boundary from coming into tension with the other two boundaries. It is hard to believe that this information is actually reviewed by any human being, more likely it is an automated process. It can of course become an issue if the information is used to perform tele-marketing or sold to a third party. The disclosure and temporal boundaries are once again in tension as in the case for data mining; by buying certain products the consumer tells the company more than likely intended about himself or herself. There is also no telling how long that information will be stored[4].

2.2.3 Positioning

The advent of *GPS* (Global Positioning System) brought us the possibility to track our physical movements geographically in real-time using special devices that communicate directly with the GPS satelites. GPS is widely used by sailors, hikers, traveling salesmen, and by anyone else who often find themselves in unknown territoris. As most GPS units can be bought by anyone without surrendering name or any other information that leads back to oneself, GPS can be regarded as quite privacy friendly. However, this is not the case with cellular phone positioning which has become a reality in recent years. Today base stations or even satelites can track our every movement using a technique known as triangulation, where signal strength measured by several satelites can be anaylzed and combined into a geographical position. This information, if stored, is a potential threat to personal privacy, especially if the user's position is determined at a regular basis[4].

It has become the habit of several car owners to hide passive radio tracking devices in their cars, so it may be found should it be stolen. Some devices can even position themselves using GPS, and even contact the owner's cellular phone should some preset conditions arise. Similar devices are used by so called "smart highways" with toll booths. A passive radio transmitter is installed into the car, which is read by the toll booth's computer as the car passes through the toll. The toll both computer may then deduct a certain amount of money from the car owner's account, or it may accumulate the transactions and send them to the owner as regular bill[4]. This is certainly an efficient process, but once again there are privacy issues that must be dealt with. The data collected by the toll booth can easilly be used to map someone's movements and subsequently used for surveillance activites. Combined with traffic surveillance cameras that can read license plates, and other intelligent traffic systems (ITS), tracking a certain individuals movements in an urban area becomes quite easy.

2.2.4 Surveillance

Surveillance comes in may forms, the most straightforward being camera surveillance. The primary use for cameras is to catch criminal actions on tape as they take place, to make the apprehension of the culprit easier, and to provide adequate evidence in court. Whether personal privacy is an issue with camera surveillance depends somewhat on the context. A bank, for instance, needs to maintain a certain level of security, to protect its patrons' assets, which is hard to do without the use of cameras. This is usually excepted, as it benefits us as customers as well. However, when public places commonly associated with social recreation are being monitored, the need for surveillance and the importance of personal privacy must carefully be weighed against eachother. You probably do not

want to be watched over while soaking on the beach, or when you go bowling. Some cases are much more difficult; take for example the museum with all the valuable works of art. To prevent theft or sabotage, museums are often riddled with cameras, but this is quite different from the bank; you as a vistor do not own anything in a museum, and a visit to the museum can certainly be considered a recreational act. Wherever you may be, there are certain times you most likely do not want to be caught on tape, such as when picking your nose, repositioning your underware, or even being there with the "wrong" person[4]. Another problem with camera surveillance is the lack of control we can exercise over the recorded material, which of course is a violation of the disclosure boundary discussed above.

2.3 Attitudes about Privacy

In this section, the findings of two independent surveys on attitudes about personal privacy will be presented. The findings are those of Cranor, Reagle and Ackerman as presented in their paper *Beyond Concern: Understanding Net Users's Attitudes About Online Privacy*[7](from here on refered to as survey A), and those of Berglund and Sjödin as presented in their paper *Storebror ser dig!*[4](eng: Big brother is watching!)(from here on refered to as survey B). The former survey, A, is mainly concerned with online privacy, i.e. privacy on the Internet, and the results are drawn from questionnaires completed by American Internet users, while the latter survey, B, has a somewhat broader area of interest including online privacy, and attitudes towards mobile positioning and customer cards. The results in survey B are drawn from questionnaires completed by people living in Sweden, which rated their concern about several privacy related issues, and also answered scenario questions related to each issue. The respondents in survey B were divided into five groups; all, men, women, young, and old. "Young" people were considered as all respondents between the ages of 26 and 35, 26 being the lowest recorded age of the respondents, while "older people" were those older that 35.

2.3.1 Online privacy

Overall, Internet users seem to be pretty concerned with online privacy, but may not always fully understand the technology they are concerned with. Attitudes towards the same technology fluctuate heavily depending on situation and context. As shall been seen, formulating a set of rules determining privacy attitudes can be very hard if not impossible.

Persistent Identifiers

Often refered to as cookies, persistent identifiers can be used to track online activities over time. When asked about cookies, roughly 50% of the respondents in both surveys indicated that they were somewhat or very concerned about them. 12% of the American respondents and roughly 30% of the Swedish respondents confessed that they were uncertain about what a cookie is. Free response questions in survey A suggested considerable confusion concerning the functionality of cookies. Many repondents seemed to believe that cookies could be used to automatically determine the user's identity even when the user had not explicitly submitted any personal data. At least one respondent believed that cookies could be used by site managers to access users' personal emails

and other personal information. When asked about the use of persistent identifier numbers, without explicitly mentioning cookies, 78% of the respondents in survey A said they would definately agree to be assigned such a number by a site, even though the described behavior of that number was identical in function to a cookie. The percentage dropped to 60% when the identifier would be used to display costumized advertisments, and to 44% if used cross-site to display costumized advertisments. Thus it appears that most of the respondents have no clear objections regarding persistent identifiers such as cookies; however, many have misconceptions about these technologies and concerns about their uses.

Email Concerns

The respondents in survey B did not seem to be overly concerned with anyone reading their private emails. They were however very concerned when asked about company directors secretly monitoring the email activities of their employees. Roughly 60% of the respondents in survey B were strictly opposed to corporate executives keeping tabs on the personal email activities of a certain employee, even if the employee in question clearly was abusing the system and neglecting his or hers work in favor of writing personal emails. However, when the employees were being monitored and also made aware of this fact, the approval rate increased significantly. Fully 60% said they did not care either way or said they were in favor. One question in survey B tells the story of two brothers in love with the same woman, and to gain an advantage, one of the brothers is employing spyware to read the emails sent between the other two. Roughly 90% of the respondents were strictly opposed to this kind of behavior, while 7-8% were neutral and 2-3% positive to the use of spyware in cases such this.

Data Mining and Profiling

According to survey B, users were quite concerned about data mining and its uses. They were however quite uncertain of what data mining actually was; fully 65% confessed to not knowing how data mining works. In fact, respondents seemed to know less about data mining than any other technology included in the survey. The authors argue that this ignorance may well be the cause for the high concern about data mining. When asked about customer profiles being kept by online retailers roughly 60% of the respondents said they were strictly opposed, while 35% said they did not care either way and 5% answered they were in favor of customer profiles.

Information Disclosure in General

Survey A found a noticeable correlation between the likelyhoods of users surrendering personal information when they could be identified and when they could not. In one scenario involving a banking Web site, 58% said they would provide financial information about themselves in order to receive online costumized financial advice. However only 35% would also supply their name and address so that they could receive the information in booklet form by regular mail. In another scenario, 84% of the respondents were willing to provide their zip code and answer various questions about their interests in order to receive customized weather information from a news, weather and sports oriented web site. When identifiable information was requested from the user, only 49% would willingly provide it.

Also introduced in survey A was the notion that some types of information or data were more sensitive than others. For example 82% stated that they were comfortable with providing the names of their favorite TV shows, while only 1% would willingly provide their social security number. Other examples include information about income (17%), medical info (18%) phone number (11%) and email addres (76%). The respondents were also asked how comfortable they would be if a child in their care between the ages of 8 and 12 were asked to provide the same information. In all cases the comfort level was lower or much lower, such as in the case of phone number (1%) and email address (16%).

It is interesting that a large precentage of the respondents were perfectly comfortable with providing their email address and age (69%), but not with provding their phone number. This could mean that getting unsolicited communications via phone is more uncomfortable than via email. In general, Internet users seem to dislike unsolicited communications. Survey A states that 61% of the respondents who said they would provide information about themselves in order to receive free coupons and pamphlets concerning interesting products would not provide said information if it were to be shared with other companies for the same purpose. However still, nearly half of those also said that they would provide the information after all, if there were some way of removing themselves from the mailing list in the future. Written comments to these questions by the respondents were quite clear on the reasons for this. As one respondent noted, "I would not want to have marketers calling me, e-mailing me, sending me direct mail, etc., as I get too much of that as it is."

Privacy Regulation and Self-regulation

One scenario in survey A dealt with a Web site with interesting information related to a hobby asking for a visitor's name and postal addres in order to provide free pamphlets and coupons. Without any further information 73% of the respondents said they definately or probably would provide their personal information under those circumstances. The resondents were then asked if they would be more or less likely to provide said information:

1. if there was a law that prevented the site from using the information for any purpose other than processing the request,

2. if the site had a privacy policy that said the information would be used only to process the request, and

3. if the site had both a privacy policy and a seal of appproval from a well-known organization such as the Better Business Bureau or AAA.

Among those who originally stated they were uncertain or said they would not provide the requested information, 28% said they would be more likely to comply if the site had a privacy policy, 48% said they would be more likely if there was a relevant law, and fully 58% said they would be more likely if there was both a privacy policy and a seal of approval. Note that this particular scenario only involved name and postal address; it is unclear how the result would turn out if more sensitive information were to be requested. Survey A also concludes that compared to the privacy policy, privacy seals are not so important criteria for determining whether or not to provide information to Web sites. The authors argue that this might be related to the general unawereness of what a privacy seal actually is and can guarantee. In one question, the names of the privacy

seal distributors were withheld, with a sharp decrease in comfort level as a result. It is likely that customers in general are not sufficiently familiar with the concept of online privacy seal programs to consider them meaningful unless they are clearly linked to a trusted organization.

2.3.2 Everyday Privacy

The following section deals with privacy issues not directly linked to the Internet. These issues follow the same pattern as online issues, in that the respondents rely heavily on context when assessing comfort level. The results described below are all gathered from survey B.

Positioning

According to survey B, mobile phone users are generally unconcerned about mobile positioning. The authors tribute this fact to the high degree of knowledge the respondents claimed to possess regarding mobile positioning technology. As another factor, they mention the possibility of avoiding having one's mobile phone being positioned by simply turning it off. They also conclude that the respondents belonging to the group "older people" are generally less concerned about mobile positioning. Scenario questions reveal that the respondents generally favor the use of mobile positioning in emergency situations, such as when locating missing persons. They are slightly less positive, but still very positive, towards the police using mobile positioning to monitor the activities of suspects. The usage of mobile positioning by parents to track the movements of their own children was also quite favorable, but less so than in the case with the police. Not quite so positive were the results when the scenario involved lovers tracking eachother activities in order to discover adultery. The least favorable scenario was that of an employer demanding the employees keeping their mobile phones switched on so that he can monitor the length of their lunch breaks.

Customer Cards

When asked about privacy concerns regarding registering of purchased goods and directly addressed commercial pamphlets due to the use of a customer card the respondents were generally unconcerned. Only roughly 16% said they were somewhat or very concerned. However, fully 50% said they were somewhat or very concerned regarding information about their purchases being sold to a third party. 46% said that it was very important for them to know exactly to what end the information gathered through their customer card would be used. Scenario questions show that while the respondents were quite positive towards receiving price-reducing coupons based on the information gained through their customer card, they were less posivite, but still slightly positive, to the supermarket being able to draw certain conclusions, such as income and number of children, from the same information. On the subject of the usage of cusomter cards leading to directly addressed commercial concerning sensitive products, such as dandruff schampoo and diet pills, the respondents were overall neutral slightly leaning towards the negative.

Surveillance

The first scenario question concerning surveillance deals with Sven who is 77 years old, lives at an old peoples' home, and can be considerd slightly senile. As he often wanders off his daughters want him to wear an electronic bracelet by which they could track him should he not be able to find his way home by himself. Over 70% of the respondents said they were positive to this, while 25% were neutral and 5% did not approve at all. Noticeable is that the group "older people" were more positive than the other groups. The authors argue that elderly people can more easily identify themselves with Sven, thus being more positive about this issue. However, the tables are turned when Sven's daughters want to install surveillance cameras in Sven's room in order to monitor his well-being. In this case 75% were directly opposed while the amount of neutral or positive respondents were equal. The opinions of the authors in this case is that this level of security does not seem to be warranted by this level of breach of privacy.

The next scenario question deals with a company using cameras and applications recording keyboard events to monitor its employees. Anders and Johan work at same company with the same kind of tasks. Anders favors the surveillance because he feels it leads to hightened productivity and good performance which is sure to be noticed by those in charge. Johan on the other hand, feels hamepered and stressed out from being watched over all the time. The opinons of the respondents are clear on this matter, fully 85% feel that this level of surveillance is not acceptable, while 10% are neutral and 5% positive. According to the authors of survey B, research has shown that job surveillance can in itself explain some work related stress, but certainly not all of it. Older people were slightly more negative compared to younger people in this question, which the authors credit to the fact that older people are certain to have more working experience than young people. In other words, older people know how a work place should, and should not, function.

Surveillance cameras in taxi cars has become a reality in recent years, and one scenario question deals with them. The question states that as a direct result of having the cameras installed, violence directed towards the driver has dropped, and fewer people leave without paying. The results show that 65% of the respondents are positive towards these cameras, 23% are neutral, and 12% are directly opposed. These results show that the need for surveillance cameras in taxi cars exceeds the level of potential breach in privacy, according to the authors. The authors also argue that those directly opposed are probably concerned with the longevity of the recorded material, and the lack of control they have over it.

2.4 Conclusions

The subject of personal integrity was often debated upon in the 1980s, but has in recent years lost some of its substance. Journalists, politicians, and scientists, which in fact are those that should actively persue questions on personal integrity, are having problems keeping up with the rapid development of information technology[4]. A question that should be asked and circulated before the introduction of any new technology should be, "For who will this new technology mean a benefit in terms of power and freedom, and for who will it not?". New technologies often have both positive and negative aspects.

However, it is very important to note that privacy does not, and should not, conflict with security. It is perfectly possible and certainly desireable to have both at the same time. The real choice, as put forward by Bruce Schneier, is *liberty versus control*[6]. Mr.

Schneier argues that the question "If you aren't doing anything wrong, what do you have to hide?" often put forward by those favouring ID checks, cameras, data mining and so on, is just as bad as the typical retort "If I'm not doing anything wrong, then you have no cause to watch me.". In both cases you accept that privacy is abouth hiding a wrong. It is not.

As we have seen, privacy is not a trivial thing. It is quite dynamic, and changes shape depending on object, subject and context. The passage of time is also a direct factor when dealing with privacy regulation. It is important to understand these facets of privacy, or Altman's *boundaries* as we have come to known them in this paper. We have also seen how many potential privacy invasion scenarios can be broken down into and described by these boundaries.

The attitudes towards potential privacy threats, as observed by the surveys presented in this paper, show us that users are far from unanimous in their evaluations regarding these threats. Age is definately involved, but does not always equate to a higher or lower degree of concern. The survey have also shown us how users that are concerned with a specific type of privacy threat are generally also concerned about other threats, which should be somewhat expected. As to the reason for this concern we have seen how lack of information, pure ignorance, and lack of control over one's own information can be a contributing factor.

This author believes that the level of technology should not bereave us of either privacy or freedom. On the other hand, it should not be hampered and held back for reasons of privacy and freedom. These things must learn to co-exist in harmony, and support rather than interfere with eachother. It is up to all of us to see this through by being more aware consumers and citizens. We should not take the easy way out and dump this on the politicians. The old proverb "Who watches the watchers?" is suddenly of more immediate interest than ever. Anyone who follows the news nowadays know about the "Patriot Act" of the United States, and the so called "Anti-social behaviour law" of the United Kingdom. What is anti-social behaviour? According to the government of the United Kingdom, anti-social behaviour is "any activity that impacts on other people in a negative way"[10]. An extremely vague definition at best, which includes everything from shooting your neighbour in the head to telling him to get of your lawn. And how are these laws enforced you wonder? By use of surveillance, in all of its forms, as sanctioned by the government.

Chapter 3

Implementation

This chapter describes the implementation of the application, which from now on will be refered to as *Vastus*, that was the aim of this thesis. The design requirements specified Vastus as a simultaneous server and client, where the client part was supposed to connect and listen to external sources, while the server part would provide game data to thin clients(or any other form client for that matter). How to actually implement game logic was left to the discretion of the author.

3.1 General overview

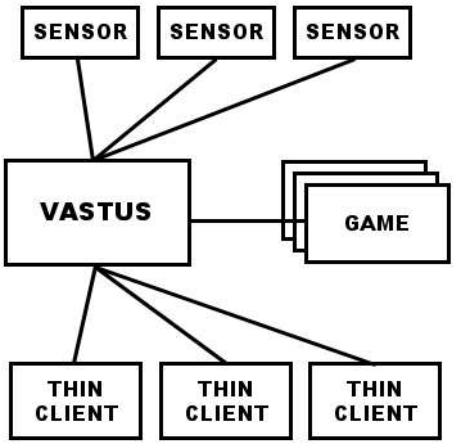

Figure 3.1: Vastus topology

Vastus is built around a simple server-client structure. The most basic unit is the *sensor unit*, which provides Vastus with sensory input, be it camera imagery, sound data, or perhaps simple user input with the mouse. The input has to be on the form of a three-dimensional matrix, not necessarily a perfect cube, of unsigned bytes. The sensors acts as servers and do not actively connect to anything themselves. Instead they are contacted by Vastus, at which time they can begin transmitting data. See section 3.2.1 for an overview over the protocol being used. Vastus can receive data over UDP

or TCP depending on the type of transmission being requested. Note that Vastus can connect to several sensors at the same time. Of course, the sensors do not actually have to be pure sensors; they can infact be other instances of Vastus masquerading as sensors. This does make any difference regarding functionality, since all Vastus needs is a stream of bytes. This also implies that a client can be an instance of Vastus, rather than only a thin client. With this architecture, several instances of Vastus can be connected together in an intricate network, effectively forming a P2P-network. However, the current implementation of Vastus does not support connections to other instances.

Received data is collected and stored in a matrix object, which is passed along to one or more *filter chains*. Each chain is comprised by one or more *filters*. These filters perform some kind of calculation on the received data. If there are more than one filter in a filter chain, they first filter receives the raw data, processes it, and then passes along the result to the next filter in the chain. The result from a filter can be of any concievable type, such as integer, floating-point number, or even another matrix. All filters expect a matrix as input, so there is no way an integer producing filter can pass along its value to another filter of any type. This means that if a chain contains a filter that does not produce a matrix, it must be the only filter in the chain or be occupying the last position in the chain. Different filters can be combined to achieve a desired net effect.

Vastus allows the dynamic loading of *games*, which must implement a predefined game interface. Vastus uses this interface to communicate with the game without actually knowing what goes on inside the game. The game is supposed to request data from the filter chains, which the game will use to control the avatar(s) in the game world. How it does this is entirely up to the programmer of the game. The game should also present the game world graphically, and is allowed to use Vastus menu bar to add menu options.

To view the game world from another site, the Vastus' *thin client* may be used. The client will contact a by the user known instance of Vastus, find out which game is currently running, and if possible load that game. It will then start to request game data packets from the Vastus instance and feed them to the game. As Vastus has no idea of how the game data should look like, it is responsibility of the game to provide methods for requesting and inserting a game data packet. These methods are part of the game interface mentioned above. Given an input or output stream, the packets must be able to receive and send themselves.

3.2 Sub-system Details

This section aims to describe the inner workings of Vastus in more detail. The main concerns here are the sensors and associated protocols, and the Vastus engine itself.

3.2.1 The Sensor

The main purpose of the sensor is to supply Vastus with sensory input on the form of a three-dimensional matrix containing byte values. There is no limit as for how the sensor collects its data. It can be computed from camera imagery, microphone input, user interaction through keyboard/mouse, amount of network traffic, or even be randomized. The data itself is transient and does not need to be saved by the sensor, i.e. if the data is not requested in time, it may be discarded. The protocol described

in the following section does not allow for Vastus to retrieve any other data than the current. Data can be transmitted using the following routines,

- **FRAME** – The sensor sends the data frame by frame, i.e. matrix by matrix, at a rate set by Vastus. No data is sent until the entire matrix has been compiled. UDP is used to transmit the data.
- **UPDATE** – The sensor only sends data when it has changed. Note that the whole matrix is sent when this happens. UDP is used to transmit the data.
- **PULL** – The sensor does not send any data unless explicitly requested by Vastus. When requested, it transmits the entire matrix. Since this service does not qualify as streaming, the data is sent over TCP to ensure its safe arrival.

The simplest way to implement an sensor of any type, is to use the SensorRelay helper class bundled with the Vastus package. This class manages incoming connections from one or more instances of Vastus. All that needs to be done is to program the data computation algorithm and feed the result to the relay.

Commands are sent to the sensor over TCP in plain text, and data is streamed from the sensor over UDP. The data is sent row-wise starting at depth 0.

Protocol

Client/Vastus Commands

- **CONNECT <UDPport>** - Used to request that the server connect with UDP to the specified port on the client machine. If the sensor is able to establish the connection, it must respond with OK(see sensor commands). In all other cases the proper fault code must be returened.
- **GET_WORLD** - Used to retrieve meta data describing the dimensions of the sensor's matrix, the maximum frame rate allowed, and the maximum and minimum value that a single cell in the matrix can hold.
- **GET_SERVICES** - Retrieves a list of the services that the sensor is offering, the answer should be a
- **GET_MAX** - Retrieves the maximum value that can be held by a cell in the sensor's matrix .
- **GET_MIN** - Retrieves the minimum value that can be held by a cell in the sensor's matrix .
- **GET_DATA** - Used to request that the sensor transmit its matrix over TCP. Usually used in conjuction with SET_SERVICE PULL described below.
- **START** - Used to signal the sensor that it should start transmitting data. The server must reply with OK(see sensor commands) or a proper fault code. This command is usually used in conjuction with SET_SERVICE FRAME/UPDATE described below.
- **STOP** - Used to signal the sensor that is should stop transmitting data. The server must reply with OK(see sensor commands) or a proper fault code. This command is usually used in conjuction with SET_SERVICE FRAME/UPDATE described below.

- **DISCONNECT** - Terminates all connections over TCP and UDP.
- **SET_RATE <RATE>** - Used to set the rate at which the sensor should stream each frame. The rate must not be higher than maximum rate returned from GET_WORLD. The server must reply with OK(see sensor commands) or a proper fault code.
- **SET_SERVICE <UPDATE | FRAME | PULL>** - Used to specify which kind of transmission type the sensor should use. The server must reply with OK(see sensor commands) or a proper fault code.
- **SET_COORD <X XDIM Y YDIM Z ZDIM>** - Used to specify a certain part of the matrix that should be sent. Data outside this range will be discarded. Note that the usage of this command should not effect the values retured from GET_WORLD.

Server/Sensor Commands

- **OK** - Sent to indictate success in response to CONNECT, START, STOP, SET_RATE, SET_SERVICE and SET_COORD.
- **WORLD <XDIM YDIM ZDIM RATE MAXVAL MINVAL>** - Sent as response to GET_WORLD. XDIM, YDIM and ZDIM describes the dimenstions of the sensor's matrix, rate is the maximum allowed send rate, and maxval and minval represent the maximum and minimum value that can be held in a cell the matrix.
- **SERVICES <SERVICE-LIST>** - Sent as response to GET_SERVICES. Should be on the following form:
  $111 \Longrightarrow$ PDATE | FRAME | PULL
  $110 \Longrightarrow$ PDATE | FRAME
  $001 \Longrightarrow$ PULL
  $\vdots$
- **PUT_MAX <MAX-DATA-MATRIX>** - Sent as response to GET_MAX. MAX-DATA-MATRIX should be a matrix with each call set to the maximum allowed value for that particular cell. The matrix should be sent as a byte-array immediately following the string "PUT_MAX".
- **PUT_MIN <MIN-DATA-MATRIX>** - Sent as response to GET_MIN. MIN-DATA-MATRIX should be a matrix with each call set to the minimum allowed value for that particular cell. The matrix should be sent as a byte-array immediately following the string "PUT_MIN".
- **PUT_DATA <DATA-MATRIX>** - Sent as response to GET_DATA. DATA-MATRIX should the current matrix, andshould be sent as a byte-array immediately following the string "PUT_DATA".
- **SERVER_ERROR <ERROR-CODE> [ERROR-MESSAGE]** - Sent whenever an error has occured in the sensor. The error-code must be supplied, but the error-message is optional. The error-code may be any one of the following,
  - **100** - The sensor does not support the service requested by the client.

- **101** - The client has sent GET_DATA to a sensor that does not support the service PULL.
- **102** - The parameters specified in SET_COORD were illegal.
- **103** - Invalid parameter(s), or wrong number of parameters were sent.
- **104** - An unknown command was received.
- **105** - Internal error.
- **106** - Could not send data over UDP.
- **107** - The parameter specified in SET_RATE was iillegal.
- **108** - START was sent before CONNECT. No UDP connection established.
- **109** - Timeout.
- **110** - Illegal UDP port(as response to CONNECT).

3.2.2 Vastus Engine

Vastus functions as a client as well as a server. As a client, it connects to one or more sensors and requests data. As a server, it listens to incoming connections from one or more thin clients, and provides these with game data. Vastus' graphical user interface (GUI) is a simple window with a menu bar, from which the user can open dialogs used to configure connected sensors, filter chains, and loading games.

Each sensor connection runs in two threads; the first manages administrative commands sent over TCP, and the second handles the UDP stream. The UDP thread will not be created until a CONNECT message has been sent to the sensor, and will exit when the connection is dropped in any way.

The server part of Vastus consists of a welcoming thread which waits for incoming connections from thin clients. When they arrive, a new thread is started to handle it. This solution scales badly, but the idea is not to use Vastus with thousands of clients. Game data packets are retrieved from the game as sent when so requested by the client.

The filter chains are where the main calculations are done. The idea of using filter chains is to combine several types of basic filters into a larger and more complex filter. For example, the data could first pass through a filter detecting changes in the matrix since the last pass, then through a smooting filter which evens out the edges, and finally through a centre-of-gravity filter which calculates the mathematical centre point in the matrix according to the contained values. All filters take as input a matrix, and outputs either a new matrix, or something else such as a number, or a tuple of numbers perhaps making up coordinates in the matrix. Which filter to use depends on the game being run at the moment. Vastus is not responsible for actually running the filters, instead the currently running game will request data as it needs it. Vastus defines four standard filters.

- **Average Value Filter** - The Average Value filter is a so-called integer filter, meaning that the end result is a single integer. This integer is simply the average value of all values in the matrix.
- **Center of Gravity Filter** - This filter calculates the centre of gravity within a matrix. The center of gravity is defined as being the point in a matrix where the overall cell value is the highest. The end result is a coordinate.

– **Relative Change Filter** - This filter saves the last matrix that passed through and compares it to the current in-matrix. The end result a matrix, where each cell contains the absolute value of the difference between the corresponding cells in the old matrix and the new in-matrix.

– **Smooth Filter** - The smooth filter evens out the values in the matrix, making each cell value more like its neighbouring cells.

When a game is to be loaded, Vastus will simply use Java Reflection to create an instance of the game main class, i.e. the class being indicated by the user. If that class is not an instance of the Vastus interface VastusGame, the game will not be loaded. Once properly instanciated, a new thread will be assigned to the game, which in turn can create its own threads should need arise.

3.3 Ping-Pong

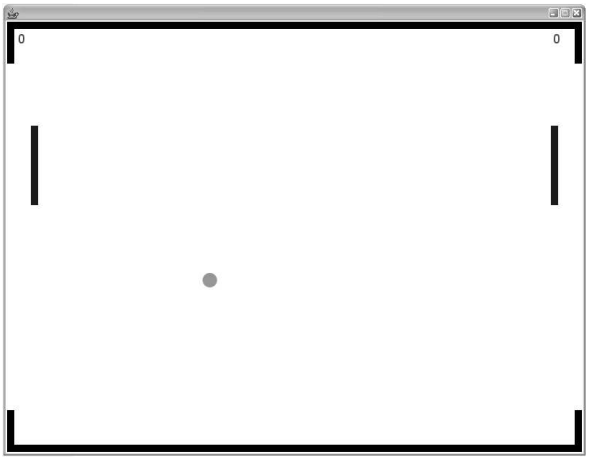

Figure 3.2: Ping-Pong running on Vastus

To demonstrate the functionality of Vastus, one game was to be implemented. The familiar game of Ping-Pong was chosen for this purpose. The reasons for this were mainly its broad familiarity, and simple nature. Furthermore, as emphasis was on the engine itself, it was prudent to pick a game that was very light on graphic and logic. Figure 3.2 shows a screen dump from Ping-Pong.

Chapter 4

Conclusion

Implementing Vastus has been a challenge. The nature of the filters and dynamic games offer small quirks that are hard to foresee during planning. However, with Java, the hardest part is always to get the layout right. My affinity with Java's layout managers is weak. At the point of this writing there has been no live test of Vastus. I look forward to discovering just how far people are willing to go just to move that paddle and hit the Ping-Pong ball. It would be interesting to see how the mentality changes as the size of the test group increases or decreases. It is prudent to assume that a single individual will be much more reluctant to letting himself go. While in a group context however, the embarrassment is in some way shared. The same goes for the intensity required to control the avatar. Slow and non-flamboyant actions could be more inviting, as opposed to quick and extravagant dito.

Working with the subject of privacy and personal integrity has been somewhat of an eye opener for me personally. Recent events in world politics have effectively furthered my interest on the matter. Privacy is a tricky thing at best. There are probably as many opinions regarding privacy as there are human beings on this planet. Still, there are some things that the vast majority of us have in common, things that by common sense should apply to everyone everywhere. Surveillance of any kind must never be allowed to become so commonplace that we forget about it and submit our lives to the authorities. Even if used for a perfectly good cause, surveillance must always be questioned. A society ridding itself of the tyranny of terror acts through heavy surveillance is still living in tyranny. As with naked violence, total scrutiny of our daily lives have to be the last resort when all other hope is lost.

Chapter 5

Future Work

Apart from rewriting the code from scratch, which would be required if Vastus was ever to used in a professional context, there are these points:

- Testing the concept live, preferrably with a larger audience.
- Reading up a little more on group dynamics in order to stage sane experiments.
- Expanding the program with additional filters more suited for other forms of sensors than cameras and microphones.
- Consulting with actual experts in the social engineering field and present them with my work.

On the subject of privacy and integrity I can safely say that I will continue to follow the debate, and do whatever I can do to help prevent what I look upon as a rather big threat to mankind. I am of course talking about the ever increasing acts of surveillance and unfounded control issued by our governments, with "national security" as the permanent reason. The least anyone of us can do is to inform those around us about the current situation, and what may happen if we do act in time.

Chapter 6

Acknowledgements

I would like to thank my supervisor, Anders Broberg, who has coached through this rather lengthy thesis. I would also like to thank my friends and family, especially my mother, who has nagged at me from time to time in an attempt to make me reach the finish line. If not for her, I would probably not have done anything so far.

References

[1] Irwin Altman. Privacy regulation: Culturally universal or culturally specific. *Journal of Social Issues*, 33(3):66–84, 1977.

[2] Anders Olsson. *Privatliv & Internet - som olja och vatten.* TELDOK och KFB, Stockholm, Sverige, 2000.

[3] Stephanos Androutsellis-Theotokis and Diomidis Spinellis. A survery of peer-to-peer content distribution technologies. *ACM Computing Surveys*, 36(4):335–371, December 2004.

[4] Berglund & Sjödin. Storebror Ser Dig! - Kartläggning av den personliga integriteten. Technical report, Luleå Tekniska Universitet, Luleå, Svergie, February 2004. ISSN: 1402-1781 - ISRN: LTU-C/DUPP–04/02–SE.

[5] BitTorrent. The BitTorrent web site. Webpage, 2005. `http://-www.bittorrent.com`.

[6] Bruce Schneier. The Eternal Value of Privacy. Webpage, 2006. `http://-www.wired.com/news/columns/0,70886-0.html?tw=wn_index_2`.

[7] Cranor, Reagle & Ackerman. Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. Webpage, 1999. `http://www.research.att.com/-resources/trs/TRs/99/99.4/99.4.3/report.htm`.

[8] Genome@Home. The Genome@Home web site. Webpage, 2005. `http://-genomeathome.stanford.edu`.

[9] Gnutella. The Gnutella web site. Webpage, 2005. `http://www.gnutella.com`.

[10] Home Office of the United Kingdom. Anti social behaviour. Webpage, 2006. `http://www.homeoffice.gov.uk/anti-social-behaviour/`.

[11] Howard Rheingold. *Smart Mobs - The next social revolution.* Basic Books, Cambridge Center, Cambridge, 2002.

[12] Irwin Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding.* Brooks/Cole Pub. Co., Inc, Moneterey, CA, 1975.

[13] KaZaA. The KaZaA web site. Webpage, 2005. `http://www.kazaa.com`.

[14] Napster. The Napster web site. Webpage, 2005. `http://www.napster.com`.

[15] Dagens Nyheter. Företagen övervakar anställda hårdare. Webpage, 2005. `http://-www.dn.se/DNet/jsp/polopoly.jsp?d=678&a=508909`.

[16] OceanStore. The OceanStore web site. Webpage, 2005. http://-oceanstore.cs.berkeley.edu.

[17] Palen & Dourish. Unpacking "Privacy" for a Networked World. In *CHI'03*, 2003.

[18] Peter Siepel. *Jurudik och IT-Introduktion till rättsinformationen*. Nordstedts förlag AB, Lund, Sverige, 1997.

[19] phpbb.com. phpBB - Creating communities. Webpage, 2006. http://-www.phpbb.com.

[20] Seti@Home. The Seti@Home web site. Webpage, 2005. http://-setiathome.ssl.berkeley.edu.

[21] C Shirky. What is p2p... and what isn't. Webpage, 2000. http://-www.oreillynet.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html.

[22] Wiki.org. What is Wiki. Webpage, 2002. http://wiki.org/wiki.cgi?-WhatIsWiki.

[23] WikiPedia. NetBus. Webpage, 2005. http://en.wikipedia.org/wiki/Netbus.

Appendix A

Vastus Usage

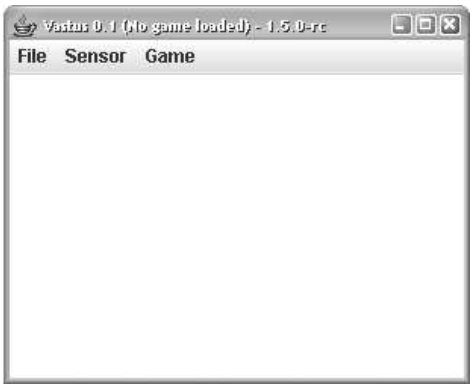

Figure A.1: Vastus main window

Before any games can be loaded, the filter chains must be set up, and before that can happen, Vastus must connect to one or more sensors. To connect to a sensor, simply open up the sensor configuration diaglog, and enter the sensor's hostname and port number and hit "Connect". If the sensor is properly configured and adhering to the Vastus protocol, it will be added to the sensor list. Vastus will automatically retrieve the world size and setup a receiving matrix object. Use the text field at the bottom to send explicit messages to the sensor that is currently selected.

Once the sensors are set up, open up the configure filter chains dialog. There are no chains configured the first time this screen is loaded so just press "Add" to add a new filter chain. In the next dialog, all available filters will be listed on the left. Add filters in turn by pressing the arrow keys in the middle. Each filter can be configured to work on a different part of the matrix, but please note that by limiting a filter's active area, you also limit the active area of the following filter, if any. In other words, the last filter in the chain can not have an active area that does not fit inside the active area of the filter before it. The filter can be renamed to better reflect what kind of filters it employs. The idea is to pick the filter that is most suited for the particular game that is to be loaded. For instance, if one sensor is a camera, it makes sense to combine the relative change filter and the average value filter. First the relative change filter calculates which cells that have been changed, and how much. The result is then passed

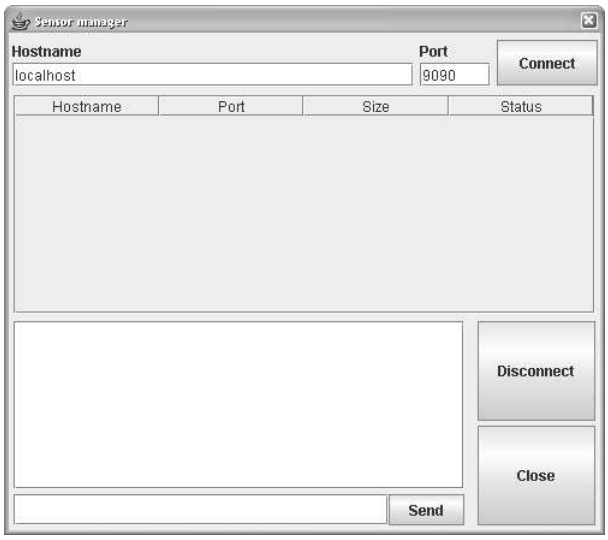

Figure A.2: Sensor configuration dialog

along to the average value filter, which calculates the average value of all cells in the matrix. The resulting integer shows, on a scale from the sensor's minimum matrix value to the maximum matrix value, how extensive the picture recorded by the camera has changed between frames. Using this type of filter chain makes it very difficult reach the maximum value since that would entail shifting all cells in the matrix from minimum to maximum or vice versa. An alternative is to replace the average value filter with the center of gravity filter. This filter chain will give the region where the largest degree of change has occured, making it quite easy to reach any value; all that is needed is the wave something in the appropriate part of picture.

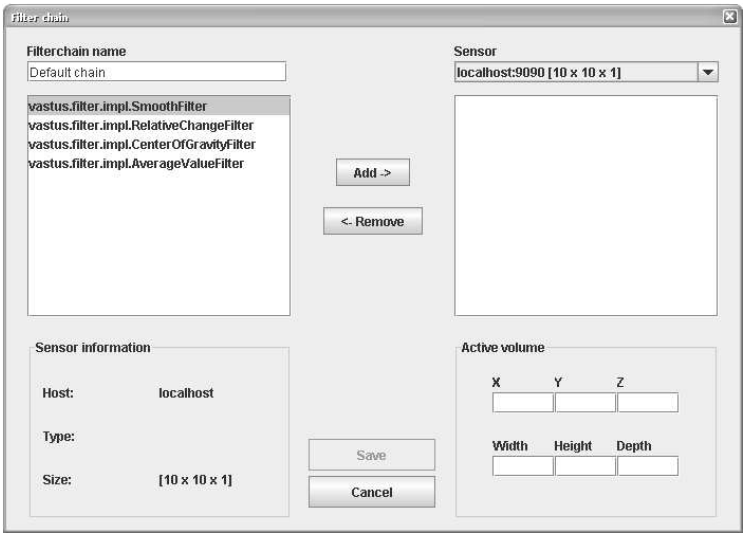

Figure A.3: Filter Chain configuration dialog

Now the game can be loaded. This can be done in two ways depending on how the game is stored in the file tree. If there is a single file sitting in the root of any of the specified classpaths, it can be loaded by opening up the file browser(**File→Boot Game**) and selecting the file. If it is stored further down the classpath, it must be loaded by supplying the package and class name(**File→Boot Game from CLASSPATH**) "java style", e.g. "mygamepackage.GameClass". Depending on the game, it will add widgets to the Vastus window or perhaps open a window of its own. Vastus holds a menu, "Game" which can be freely used by the loaded game to add menu options.

Appendix B

How to Write a Game for Vastus

Any game that is to run in the Vastus environment must implement the interface `vastus.VastusGame`. A short description of the methods follows.

- `initialize` – Initializes the game. Will be called automaticaly when game is instanced.
- `setRunning` – This method should implemented to start/stop the game.
- `getDataPacket` – This method should return an instance of a game-specific data package class that inherits from DataPackage. This package should contain all information necessary to paint the current scene on a client. It is the users responibility to design, implement, and use this class. Vastus vill query this method regulary and send the result to any connected client.
- `getEmptyDataPacket` – This method should return an instance of a game-specifc data package class that inhertis from DataPackage. This class should be of the same type as that being returned in getDataPacket(), but it should be empty.
- `useDataPacket` – This method will only be used on clients. When called, this method should extract the information from the supplied packet and paint the scene accordingly.
- `getName` – This method should return the name of this game.
- `getConfigStrings` – This method should return an array of strings representing the game's configuration. This information will be passed along to any connected client. It is the user's responsibility to design these strings; Vastus itself will not use or parse these strings in any way.

How the game actually displays its scene is the user's responsibility. The main window can be reached through a call to `Factory.getMainUnit().getMainWindow()`. The game is free to draw things in this window, although it is advisable to open a separate JFrame for moving graphics. The main windows also has a menu dedicated to which ever game is running. This menu can be fetched through a call to `Factory.getMainUnit().getMainWindow().getGameMenu()`. The user is free to add JMenuItems to this menu.