

Spam on the phone - VoIP and its biggest weakness

Studies about the users' willingness to offer personal
information in order to avoid VoIP spam

Daniel Putz

Abstract

It is very probable that VoIP will soon replace the ordinary telephone. Beside all advantages of the digital voice-connection it is linked to the danger of spam on the telephone. A lot of approaches have been developed to solve the problem of VoIP spam. Because some of these solutions are based on access to personal information of its users, a broad discussion about the best and most ethical approach has started.

This thesis analyzes the users' point of view towards the VoIP spam problem and the extent of users' willingness to offer private information in order to avoid VoIP spam. It presents results from a qualitative and a quantitative research as well as approaches for a most realistic- and most promising VoIP solution. These new approaches are based on the results of the research.

The main points of the results showed that users were not willing to offer private information to companies and that they were not willing to pay any amount of money for VoIP spam solutions. Users held governmental organisations and telephone operators responsible for finding a solution against VoIP spam.

Keywords

VoIP, spam, SIP, H.323, HCI, telephony, privacy, ethics, filtering, authentication, pay-per-call, digital signatures, Turing test, commercial, advertisement, IP-telephony, RFC 3261, Spitz, VAM, Skype, MSN-messenger, Sipgate

Table of content

Abstract	2
Keywords	2
Table of content	3
1. Introduction to the topic	5
1.1. Spam, a modern problem	5
1.2. VoIP Spam	6
1.3. Aim of the study	6
1.4. Background	6
1.4.1. Why is the research necessary?	6
1.5. Spam solutions – advantages / problems	7
1.6. VoIP spam research – how to do, what to expect	7
1.6.1. Differing between “VoIP spam (un)experienced” users	8
1.6.2. Why use a “Voice Commercial” – prototype	8
1.7. Hypothesis	8
1.8. Limitations	9
1.9. Outline	9
2. Theoretical foundation	10
2.1. VoIP telephony	10
2.2. What is spam?	10
2.3. VoIP spam from the technical point of view	11
2.4. What kinds of VoIP spam solutions are available?	12
2.4.1. Filtering at the receiving end	13
2.4.2. Using “white lists” or “black lists”	13
2.4.3. Authentication	14
2.4.4. Digital signatures	14
2.4.5. Pay-per-Call	14
2.4.6. Turing Tests	15
2.4.7. (Dis-)Advantages from the users’ point of view	16
2.4.8. Personal Information users have to offer in order to make solutions work	16
2.5. The myth of users’ need for absolute privacy	16
3. Methodology	18
3.1. General structure of the research	18
3.2. Target Group	18
3.2.1. Persona as an Example	19
3.3. Qualitative Research	19
3.3.1. Guidelines for the interviews	19
3.3.2. “Voice Commercial” – prototype	22
3.3.3. Field of application	23
3.4. Quantitative research	24
4. Results / Discussion	25
4.1. Overview	25
4.2. Description of test users	25
4.3. Analysis of research data	25
4.3.1. Analysis of qualitative research	26
4.3.2. Answers to quantitative research in comparison	27
4.4. VoIP spam psychological component	30
4.5. Analysis of research results in relation to VoIP spam solutions	30
4.6. Spam solutions in relation to the research	31
4.6.1. Most realistic VoIP spam solution	31

4.6.2.	Most promising VoIP spam solution	32
5.	Summary and Conclusion	35
5.1.	Validity / Reliability	35
5.2.	Comments	36
5.3.	Further research	37
5.4.	Summary	37
	References	38
	Appendix	41
	Appendix A: Guideline for the interviews on the qualitative research	41
	Appendix B: Questionnaire for the quantitative research	42
	Appendix C: Texts Voice Commercials.....	44

1. Introduction to the topic

This chapter provides an introduction to the thesis, its background and the question why the thesis is needed and is useful. It will give a short introduction to the different problem domains, will also guide the reader through the different advantages and problems of its solutions and it discusses the limitations of the thesis. The Outline section gives an overview about the whole thesis and leads the reader to the theoretical foundation.

1.1. Spam, a modern problem

Nowadays nearly everyone in Sweden, probably everyone in Europe, uses email as a means of communication or knows at least what an email is. Since the technique of sending an electronic mail was invented it has grown tremendously. The technique became widely accepted and even succeeded to replace the letter as the usual means of communication.

The technique of Voice over Internet Protocol (VoIP) has ambitions to replace the telephone in the same way email replaced the letter. Since broadband became common it is possible for everyone to transmit calls over the internet. And companies such as Skype (Skype, 2007), MSN-messenger (Microsoft-corp, 2007) or Sipgate (Sipgate, 2007) are very successful in selling VoIP services. But beside all the positive facts the different techniques face a lot of problems which need to be solved. The biggest problem and thereby the biggest weakness of the new techniques is spam.

It is important to take into account that there are a lot of different types of spam. The most well-known type is email spam. Users receive a lot of spam emails each day and use filters and black-lists to filter out as many of them as possible. While VoIP is using a similar technique (for transmitting information) to the one for email, it seems to be quite obvious that VoIP will face the problem of spam as well, but in a different and much more intense way. And that is the big weakness of the technique of VoIP. While an email can be easily filtered and deleted, a call is much harder to identify. And while an email can be received asynchronously a call needs to be received synchronously and is therefore much more annoying for the user.

Even though VoIP is still in an early stage and VoIP spam actually does not even exist today, it already seems to be clear that the spam flu will spread and infect the internet telephony, too. Accelerated by globalization and the need to get connected all over the world by reducing the price permanently, the pressure on developers for VoIP is high. And in order for internet telephony to be accepted, a solution for the upcoming spam problem is needed. But it needs to be a solution that is accepted by its users, if VoIP wants to succeed on a wide range. And here a VoIP - 'internal' problem occurs. A discussion within the VoIP-community is taking place about which solution may be the best one, which kind of technique is acceptable and who shall have the right to develop it (IETF, 2007). Sadly this discussion makes the ambitious developers forget about the end user, the ones the solutions are built for, and becomes a subjective, ideological fight.

This thesis discusses the different solutions against VoIP spam (following called VoIP spam solutions) and its disadvantages from the users' point of view. The thesis then turns to the question of what kind of private information users are willing to offer in order to avoid spam. An analysis on this question discusses the users' point of view. At the end of the thesis the result of this analysis is presented that offers information about the users' point of view about the different VoIP spam approaches.

1.2. VoIP Spam

Many people have never heard about “VoIP spam”. Even if they use internet telephony, they have probably never heard the term “VoIP” either. This is not important due to the fact that these terms are of technical nature and not everybody needs to know about them. People understand if someone is talking about internet telephony or telephone spam. Every user has a certain idea about what spam is; mostly due to the fact that they receive quite a lot of email spam. When talking to people about telephone spam they can imagine what it could be but do not actually know what it is. When explained that it is, e.g. a call from a reseller, they understand and can imagine that such a call could have an impact on their life. I am now already giving an idea to the reader about VoIP spam. But what is it actually? Or, furthermore, what is the difference between spam and VoIP spam?

Spam is a broad term. One needs to differ between email spam, web spam (spam on websites), IM spam (spam on instant messenger), and VoIP spam. Spam is commonly known as “unwanted text messages that contain commercial content”. But this definition cannot be applied to VoIP spam. That would be “unwanted voice messages that contain commercial content” while the definition is not as focused as it should be. A telemarketing call may not be commercial while still unwanted and may be defined as spam. But is it actually spam? As one can see even the definition of VoIP spam is quite vague. It is not surprising that every-day-people do not have any idea about what VoIP spam is. This will cause a problem because users may not take into account the possibility and problem of spam while changing from traditional telephone to VoIP. It is important to inform people about the upcoming problem of VoIP spam as well as it is important to develop VoIP spam solutions. Only if there are good solutions against VoIP spam available, the new technology of VoIP will be accepted. And only if people are informed about the problem they will accept to offer information in order to avoid VoIP spam. In chapter 2, Theoretical Foundation, a definition of VoIP spam is given that shall be taken as a basis for this thesis.

1.3. Aim of the study

This thesis analyzes the users’ point of view towards the VoIP spam problem and the extent of users’ willingness to offer private information in order to avoid VoIP spam. The research shows what the main target group of users wants. On the basis of that, an argumentative base for pro and contra for further discussions about VoIP spam solutions is provided.

1.4. Background

This chapter introduces some background facts about the research and the problem domains. It provides the reader a picture of the reasons for the research and the differentiations and problems during the research.

1.4.1. Why is the research necessary?

A lot of people of the internet community are taking part in the ongoing discussion about a well formed approach for VoIP spam. The continuous problem of handling email spam and having no appropriate solution to the problem makes specialists doubtful if there ever will be an appropriate solution for VoIP spam. In fact, the problem is not so much the search for a proper solution but a question of attitude.

There are different solutions to VoIP spam which seem to solve the problem quite satisfactory and seem to be adequate solutions. Various companies have already shown that their products can handle the problem of VoIP spam quite well by using various techniques. Other solutions are until now based on theories only, but already promise quite efficient

results. It is a fact that these solutions depend on registrations, user tracking and various other facts that may reduce people's anonymity on the internet. While different spam professionals view this reduction of freedom as acceptable, thinking it to be the lesser of two evils, many internet idealists view this reduction as an act against the idea of the internet itself. They fear that a reduction of freedom may change their basic idea of the internet and reduce their right to free information exchange. Thus the discussion about a proper VoIP spam solution becomes less objective and the actual problem is overlaid by a dispute of attitudes. In this case, the question of whether a solution could actually solve the problem can thus no longer be answered objectively. But, in order to keep VoIP spam at bay, it is important not only to think of a solution to the problem but also to develop proper tools for it as well. In order to achieve this goal an acceptable answer for a wide audience needs to be found. This is only possible through the gathering of information of people who use the media of telephone daily and will also use the technology of VoIP in the near future.

Therefore, by experience and by evaluation, VoIP spam is already viewed as a problem in the near future; and it will occur the moment VoIP will be used on a wide market.

1.5. Spam solutions – advantages / problems

Because VoIP spam solutions will become so important a couple of different approaches have already been developed. Most of these approaches were designed for email spam but re-thought for VoIP spam. The main difference between email spam and VoIP spam is the kind of reception. A call needs to be answered synchronically and is thereby more annoying than email spam. Thus, VoIP spam solutions need to be better than standard email spam solutions because of the level of annoyance.

The most commonly used technique is to filter information and see if it is spam or not (See chapter 2.4.1). A similar solution is based on black- and white lists (See chapter 2.4.2). Other solutions are based on authentication of sender and receiver (See chapter 2.4.3 and 2.4.4). Moreover, there are also solutions that take a fee for every message into account (See chapter 2.4.5).

There are different approaches which are built on different preconditions. The preconditions are mostly linked to users' personal information. Some solutions try to keep the users' privacy to 100% while other solutions use users' personal information to authenticate sender and receiver in order to facilitate tracking spammers.

The different types of solutions stir up a lot of discussion about ethical behaviour and privacy of communication. These discussions have a serious impact on the development process of spam solutions. The argumentations for good or bad solutions become weak and non transparent.

1.6. VoIP spam research – how to do, what to expect

Every developer has his reasons why his solution is the best one and why his solution will be the most accepted one.

But when developing a solution for the mass market it is important that such solution becomes widely accepted. A solution that is developed out of a subjective point of view will probably not succeed. This is especially true for spam solutions. Due to the fact that different solutions require different information, some solutions may infect the users' privacy while others do not. An important fact to take into account while discussing solutions against spam is that a possible solution will influence the way of communicating on the internet. Thus, it will probably alter the general 'idea' of being anonymous on the internet, because people may need to offer personal information in order to avoid spam. Moreover, some companies have commercial interests that influence the discussion as well.

The acceptance of every spam solution is influenced by the discussion on whether users should be forced to offer personal information or not. Some groups want to protect the anonymous internet and do not want to disclose any personal information to anybody; one group is the Electronic Frontier Foundation, EFF (EFF, 2007). These groups are quite powerful because they are seen as the advocates for a free and independent internet against the government and some companies which want to regulate the internet. Solutions that do not fit the idea of these lobbyists have a hard time to get accepted. On the other hand there are some companies which have a huge influence on the internet and its solutions. They have a more commercial purpose.

As one can see the problem which occurs, taking these discussions into account is that a good solution may not be accepted due to the given discussion. The users' point of view is no longer taken into account than the interests of the different discussion-groups command the way the solutions shall be developed.

1.6.1. Differing between “VoIP spam (un)experienced” users

One goal of the research was to explore “how users experience VoIP spam” and “how and if they are annoyed by it”. The definitions of telephone spam used in this thesis are expanded to include telephone commercials, telemarketing etc. (either VoIP or ordinary phone, mobile phone).

Thus, many of the test users have never encountered telephone spam before and hence did not have any idea about the extent to which such calls would influence their daily life and behaviour of telephone use. These test users were confronted with spam calls that were produced in relation to this research. Some test users had already experienced spam calls before. In order to not overly irritate them with even more spam (even if it was fake spam), it was differentiated between the ones who were permanently confronted with it and those who have never experienced it at all.

See chapter 3 for more information regarding the research method.

1.6.2. Why use a “Voice Commercial” – prototype

Because VoIP spam actually does not exist yet, researching and questioning users about their opinion in this area cannot be conducted. Some test users had an opinion about VoIP spam beforehand. Even though the research showed that these test users changed their point of view the moment they actually were confronted with the problem. In order to illustrate this, think about a conversation with anyone; about disturbance by loud music. During the discussion you will surely agree that you would, in general, not be disturbed by loud music. But the moment you get home, want to sleep and your neighbour plays music with bass (it does not even need to be loud) you will feel disturbed and after a short while you will be quite annoyed. And you will want to stop your neighbour from playing loud music. Well, this surely is an extreme example but nevertheless a quite realistic one. VoIP spam calls as well disturb people's daily life and even the test users did not realize it before, they realized it the moment they were confronted with it. And they became really annoyed by telephone spam (See section 4.3).

1.7. Hypothesis

The main goal of this research and of any research is, and should be, to gather information objectively. The research questions are based on previous researches and results and try to avoid leading in any direction. Nevertheless there is always a hypothesis regarding a research.

People are afraid to offer information of any kind as well as they do not want to disclose information if not absolutely necessary. No one would offer private information to anyone on the street. Similarly, no one would pay for something that is actually for free. People will not offer any private information nor pay for any VoIP spam solution as long as they have not actually experienced VoIP spam. The target users for the research underestimated the problem of VoIP spam and set their preferences at the certain moment when they were asked. The hypothesis for this research was that users are willing to offer any private information in order to avoid telephone spam, because the level of annoyance is quite high. Surprisingly enough, they insisted on keeping their private information for themselves, even they experienced telephone spam as very annoying. The hypothesis that users would offer some information and pay any price in order to avoid spam could not be verified, however, it showed interesting results in that users were very creative in combating spam.

1.8. Limitations

In order to limit the scope and efforts of this thesis the following parts were not considered:

- Legislation and law enforcement. The paper does not take into account how the legislation and law influences the topic of VoIP spam.
- VoIP spam solutions. The paper deals with the most promising VoIP spam solutions. Because of the sheer quantity of solutions and approaches it is not possible to take all of the approaches into account. The thesis discusses the most promising papers.
- New VoIP spam solutions. It is not the purpose of this thesis to present a new VoIP spam solution. The thesis presents some suggestions but it does not focus on developing a new solution.
- Spam on traditional telephone. This thesis takes only the problem of VoIP spam into account and not spam on traditional telephone.

1.9. Outline

The following chapter discusses the thesis from the theoretical point of view. It defines the term VoIP spam before it discusses the different VoIP spam solutions while taking into account the personal information users have to offer, in order for the different solutions to work as well.

The thesis then turns to the research and envisions the reason for it. It discusses why the research is necessary, what the expectations there are and what kind of problems might occur. Moreover, it gives information about the background of the topic and the research of this thesis. The methodology section explains the way the research took place and defines in greater detail what the research looked like, how it was structured and what research methods were used. Afterwards the research itself is presented. The research results are described later on in chapter 4, results and discussion. The chapter discusses the different research there is and its results. It describes the different conclusions that were drawn in relation to the research, describes surprises and puts all results in relation to the different VoIP spam solutions. Finally, the most accepted solution shall be evaluated. Chapter 5, summary and conclusion, sums up the thesis and discusses further research in relation to the thesis as well as it reflects upon the research and summarizes the results.

2. Theoretical foundation

This chapter analyzes the problem domain in theory by discussing scientific research related to this paper. The theoretical foundation shall introduce the field which the analysis is placed in.

2.1. VoIP telephony

This thesis discusses the problem of spam on the internet telephone. In this chapter I will give a short introduction to the Voice over Internet Protocol (VoIP), what its advantages and disadvantages are and how spam is related to that topic.

Varshney et al (2002) describe VoIP as follows:

VoIP involves sending voice transmissions as data packets using the Internet Protocol (IP), whereby the user's voice is converted into a digital signal, compressed, and broken down into a series of packets. The packets are then transported over private or public IP networks and reassembled and decoded on the receiving side. Residential customers can connect to IP-based networks by using the local loop from the PSTN or high-speed lines, including ADSL/DSL and cable modems.

VoIP became popular when internet broadband connections became common and it became possible to have a voice-chat in real time. Applications such as Skype (Skype, 2007) or MSN-messenger (Microsoft-corp, 2007) helped to make the technique a success. Especially Skype with more than 100 million users in 2006 made internet telephony popular. Besides Skype and MSN-messenger many VoIP providers were established, most of them using SIP protocol (Session Initiation Protocol), a standardized protocol for internet telephony.

It is important to state that different providers use different protocols. The standard of RFC 3261 is SIP which is one of the most important ones (Varshney et al, 2002). Skype, as one of the global players in internet telephony uses its own standard but have already announced that they will be starting to use the SIP protocol in 2008. The switch to SIP would push the VoIP business tremendously since a connection between Skype and ordinary SIP phones would be made possible in that case; as it is not yet possible of today to connect the Skype protocol and the SIP protocol.

It is important to state that this thesis deals only with the SIP protocol, due to the fact that it is a standardized protocol and independent from any company or platform.

The most widely used argument for internet telephony is the price. Due to the fact that nowadays nearly every internet user has a flat rate, and every call between two computers is for free, users can call for free. Moreover, a user can be reached on one number everywhere in the world without additional charge (Varshney et al, 2002).

2.2. What is spam?

I have already mentioned spam in the chapter introduction. In order to clarify the meaning I want to define the term spam and as well the term VoIP spam; although it is very difficult to define. Spam is commonly known as "unwanted text messages that contain commercial content". But this definition is quite vague due to the different area of application. As Judge (2003) says

The definition of spam is neither clear nor consistent across different individuals or organizations. Loosely speaking, we can describe spam as unwanted e-mail messages.

These types of messages are often referred to as ‘unsolicited commercial e-mail’. (Judge, 2003)

While Judge defines spam as only applying to email-messages, spam in a more general sense of the word can be described as “unwanted messages in any way”, due to the fact that spam may not only occur on email inboxes but on instant messengers, telephones, websites or anywhere else a dialog is taking place as well.

Thus, here the problem of the definition of spam occurs. The term spam commonly used for unwanted email messages but describes as well text messages on websites or voice messages on the telephone. Judge recommends

A good approach to this problem is to define the different categories of messages that may be deemed spam and allow organizations or individuals to create an appropriate definition for their environment. (Judge, 2003)

The definition for spam that is used for this thesis is the following: “Spam is unwanted messages from senders the receiver does not know”. This definition does not cover every possible scenario but it contains the needed information. By defining it as unwanted messages the definition leaves open if it is a text-, voice message. By defining that receiver do not know the sender, it limits unwanted personal messages according to personal opinion. A known sender may send unwanted messages, e.g. a joke message; but because the sender is known the receiver is able to stop these mails by contacting the sender. This is not possible for spam mails from unknown senders.

Due to the fact that spam describes unwanted messages on every platform it is essential for this thesis to define spam on the telephone; VoIP spam. VoIP spam is widely known and described as

SPIT (spam over Internet telephony), sometimes known as vam (voice or VoIP spam), is unsolicited bulk messages broadcast over VoIP (Voice over Internet Protocol) to phones connected to the Internet. (TechTarget, 2005)

The definition for spam that was stated beforehand is quite similar to the one from TechTarget. In order to make the definition clearer, it is stated that “VoIP spam is unwanted calls from senders the receiver does not know”.

The different kinds of spam need to be addressed differently. The most common ones are email spam, Instant Messenger spam, VoIP spam and Web spam. In this thesis, the term spam is used as a general term for all kinds of spam and it will be specified for the different types of spam where appropriate.

2.3. VoIP spam from the technical point of view

Since the problems of VoIP spam have already been addressed in the last chapters, this chapter focuses on how VoIP spam actually looks like from the technical point of view. In order to be able to explain this, it is first necessary to explain how VoIP, and with that, the SIP protocol actually works.

VoIP is based on the idea of sending large amount on digital data. Different from a traditional analogue telephone system, the voice here is cut down in different packages. These packages are sent to the receiver and then put together again. This happens in real time, a user does not realize that such process is happening as long as the bandwidth is high enough (Sherburne et al, 2004).

There are different protocols available which can establish such voice transition. The standardized ones are H.323 (ITU-T, 2007) and SIP (IETF, 2007). While H.323 is based on ISDN-connections, SIP is based on HTTP and therefore SIP is nowadays most commonly used (See figure 2.1).

However, VoIP nowadays becomes more and more accepted while it still suffers from some connection problems. Therefore, the main target group are still people that have technical skills. During the last few years a lot of companies selling VoIP services were founded. Anyone can connect anywhere to the internet and call with a simple application. It is expected that the amount of users will increase dramatically during the next years (Sherburne et al, 2004). And here the issue of VoIP spam comes up.

As SIP numbers work nearly the same way as email addresses, it is easy for detection software to locate a SIP telephone simply by randomly calling numbers. Since a call can be established for free by any computer which is connected to the internet, and since the bandwidth of today's internet connections allows sending many calls simultaneously, a sender nowadays can send many calls from anywhere at any time - for free. Additionally, using commercial messages instead of voice is made very simple by playing a record the moment a receiver answers the phone. As I have already pointed out, even someone new to the field of sending commercials on the phone, is able to send spam calls to unsuspecting receivers.

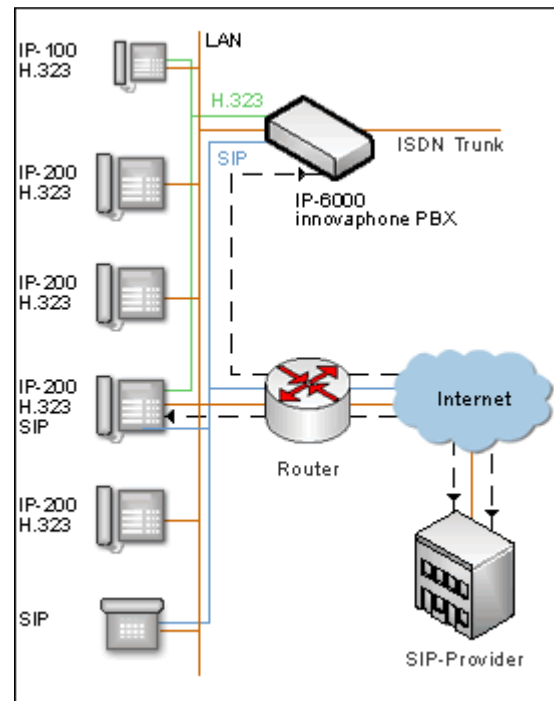


Figure 2.1: Sip and H.323 © ITM GmbH

2.4. What kinds of VoIP spam solutions are available?

Due to the fact that the areas of (traditional “email”) spam and VoIP spam are so close to each other, solutions invented to avoid spam are adopted by the VoIP companies to solve the VoIP spam problem. Most spam solutions are built on filtering systems which compare different mail patterns and sort out the dubious ones (Arrison, 2004). But, even when the solutions that are used to avoid spam nowadays are quite effective they do not seem to be adequate enough. Despite the fact that a user accepts ten spam-emails a day, he probably will not accept ten VoIP spam calls a day. That leads back to the fact that users have to answer a call synchronically while they can react non-synchronically to emails. The need to answer synchronically makes a VoIP spam-call much more annoying and thus user find this unacceptable.

Therefore, it is important to develop a solution against spam which is much better than the solutions already given and/or adapted by the discussion around the problem of spam. Indeed, to reach the goal of avoiding VoIP spam, email spam and Instant-Messenger-spam to 100%, other solutions than simple filtering solutions are needed. A discussion was started not only about which system might be the most effective one, but also about which one might be the most accepted one, the easiest to implement, and so on (IETF, 2007). Due to the fact that the different types are used to avoid different kinds of spam, it is important to consider that this thesis focuses only on VoIP spam and thus leaves out any information unrelated to this topic.

Below, the most useful solutions for VoIP spam are described. Cerf (2005) described them as the most promising solutions for the future.

2.4.1. Filtering at the receiving end

Filtering content and comparing content-patterns to other ones (in order to recognize spam) surely is one of the most commonly used spam techniques (Arrison, 2004). This solution has its origin in filtering emails and sorting out emails that include “bad patterns” (See figure 2.2). Due to the fact that every content provider has had the possibility to implement such a system in a short amount of time and the fact that this technique was successful it became the most widely used technique for email spam. There are many different VoIP spam-filtering-techniques available and many papers were written describing different approaches how to avoid VoIP spam (Cerf, 2005; Gburzynski et al, 2004).

Advantages: The advantage of using a filtering technique is that every provider, as well as every user, can implement such a technique on their system. Thus, the receiver as well as the sender of such call can stay private and does not need to disclose any personal information to anyone.

Disadvantages: Every email-user knows about the disadvantages of filtering systems; they do not filter every spam email. The problem lies in the nature of a filter; a filtering system is only as good as spam emails are bad. As Arrison (2004) states:

Filters are a little like chaperones at a teenage party. They often misinterpret legitimate actions (false positives) and they sometimes miss the naughty behaviour (false negatives). And spammers are a bit like teenagers, who will change their strategies to foil the watchers. (Arrison, 2004)

In addition to that, filters suffer from the problem that they never are up to the current technical standard of spammers. When a spammer uses a new method the filter needs to be updated to the newest methods. And until this has happened, the new spam will slip through the filter. “Filtering remains a useful if not entirely effective tactic (Cerf, 2005).”

2.4.2. Using “white lists” or “black lists”

Using the technique of different lists which recognize senders and receivers is often used in addition to filter techniques. The reason for this is that both techniques are able to operate simultaneously without interfering with each other. The method of using lists is quite simple. Two lists are used to identify “good and bad” senders (See figure 2.3). The lists contain caller-IDs or email-addresses of the senders. Calls/emails with sender-addresses from the white lists pass through the filter; calls/emails with sender-addresses from the black lists are deleted (Gburzynski et al, 2004; Arrison, 2004).

Advantages: The advantages of such a solution are similar to the advantages of filtering systems. An advantage is indeed that this technique does not allow unwanted senders to call. Other calls and mails are blocked even when they are based on the newest techniques.

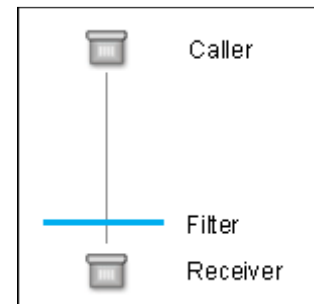


Figure 2.2: Filtering at the receiving end

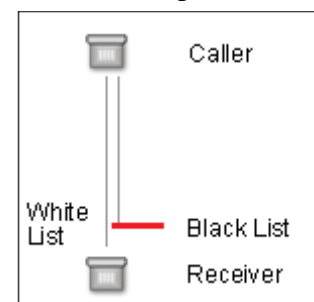


Figure 2.3: Using white- and black lists

Disadvantages: Even though the technique may have some advantages, it nevertheless has an enormous disadvantage. Due to the fact that spam email senders use different domains and thus different email addresses a problem occurs which also occurs when using filtering techniques, this technique only works properly as long as a mailer address, or number, is registered. All emails which are registered on a black list were deleted, but when a spam message is sent, which is not yet registered as a spam address, the mail gets through to the receiver. Until this address is registered as “spam address” all messages from this address get through (Gburzynski et al, 2004). Senders of spam messages therefore change email addresses all the time and generate new ones. Moreover, they are able to use the same trick for telephone numbers and generate numbers automatically. Because of this huge advantage for the spammers, this solution cannot be viewed as an effective solution against VoIP spam.

2.4.3. Authentication

This approach authenticates every user to a central organisation (See figure 2.4). When a user sends an email the receiver has the possibility to check whether the sender is registered or not (Cerf, 2005). This approach can be compared to a registered car. As long as you know the registration number you can track down the driver.

Advantages: The fact that users are authenticated makes it possible to track every sender. Therefore it is obvious that, if a spamming incident occurs, the spam cannot only be blocked but the sender can be tracked and, if possible, be made liable for the damage. This method probably is one of the most effective techniques to avoid spam.

Disadvantages: Due to the fact that a user needs to be registered to any organisation, company or governmental organisation there will not be any private users anymore. This is the main discussion and one of the main arguments against this technique.

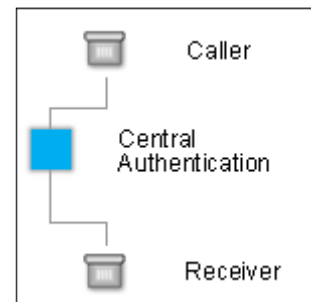


Figure 2.4: Authentication of users

2.4.4. Digital signatures

This technique exchanges a signature between sender and receiver. There are different techniques on how to exchange these signatures; but the most common technique is to exchange it through third parties; as it is shown in figure 2.5(Arrison, 2004).

Advantages: Only messages from trusted senders are accepted. People without a digital signature cannot send an email.

Disadvantages: The system needs to trust third parties. But there is no way to verify that third parties can be trusted. Thus, the system is flawed when it comes to untrustworthy parties. Only a central organization can make sure that a sender is trustful (Arrison, 2004). A spammer may use a “second party” that authenticates a third party every time he sends spam messages.

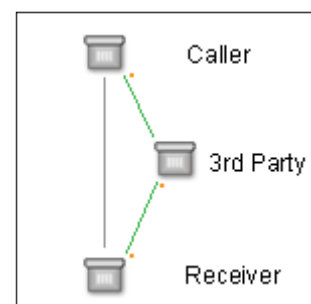


Figure 2.5: Digital signatures

2.4.5. Pay-per-Call

This technique is based on the idea that a receiver gets paid for every message that is not wanted. Every sender is charged for a spam message. Only senders which are on a non-charge list are not charged.

Family and friends would be put on the do-not-charge list and their emails would arrive in the user's inbox for free. But for anyone the user doesn't know, a charge of \$ 5 (or whatever price the user wanted) could be levied. (Arrison, 2004)

The money is put in a virtual deposit box and in the moment the receiver says "this email is spam" he gets the money out of the virtual deposit box. If the email was not spam, the money is sent back to the sender (See figure 2.6).

Advantages: Only messages from trusted senders are accepted. For every other email the user gets paid for receiving VoIP spam messages.

Disadvantages: The disadvantages that were discussed in the digital signature solution apply here as well. Another problem might be that users abuse the system and charge users who do not have the intention to spam.

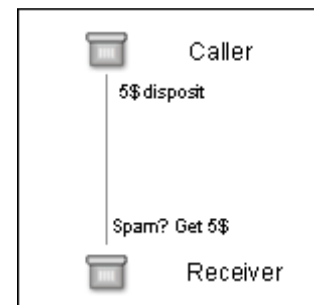


Figure 2.6: Pay per call

2.4.6. Turing Tests

The Turing test was developed by Alan Turing in 1950. It tests whether the receiver on the end of the line is a computer or a human being. There is even a yearly contest, called the Loebner-contest, about a computer (program) which is not recognized as a computer but as a human. Up until today, no computer has passed the test; all of them were recognized as computers. So called Human Interaction Proofs (HIP) are built on the basis of Turing which shall "tell humans and computer apart" and help to identify whether interaction with a computer or a human is taking place. Very popular are CAPTCHAS, Completely Automated Public Turing test to tell Computers and Humans Apart, which are commonly used on websites to confirm actions. By using CAPTCHAS it can be made sure that a human and not a computer perform the action on a website (e.g. filling out a form). There are different approaches available on using CAPTCHAS as a technique against email- and telephone spam (Goodman et al, 2007). Using a Turing test as a VoIP spam solution shall make sure that the sender is a human and not a computer. On doing so, a spamming machine can be recognized and blocked (Gburzynski et al, 2004).

Advantages: It can be guaranteed that a sender is a human and not a computer.

Disadvantages: Due to the fact that manpower is quite cheap in emerging market countries it makes no difference if a computer or a human sends a spam message. The Turing test can easily be passed by a human and then it directly passes on the receiver to a voice recording with the spam message. Another disadvantage is the fact that many companies use calling-machines for their services. Their business would be destroyed by such filtering system and their lobby would not accept any of these filtering systems (Gburzynski et al, 2004; Rosenberg et al, 2004). By using CAPTCHAS, the most commonly used technique, a research group of the University of Berkeley and the Simon Fraser University of Burnaby already proved that CAPTCHAs can be detected and recognized by computers (Mori et al, 2003).

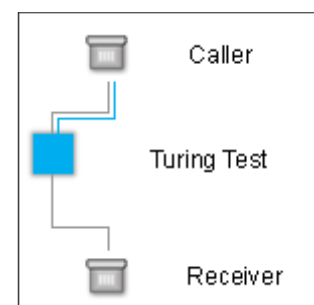


Figure 2.7: Turing test

2.4.7. (Dis-)Advantages from the users' point of view

As already stated before, the different spam techniques have different advantages and disadvantages. Due to the fact that this thesis explores the users' point of view, special emphasis is placed on the user related concerns.

The different spam detection techniques can be divided into different groups. There are solutions which protect the anonymity of users while other ones focus on authenticated users (Cerf, 2005; Arrison, 2004). The approach to authenticate users is often harshly criticized by some groups of the internet community; such as the Electronic Frontier Foundation (EFF, 2007). Their aim is to keep the users' anonymity. While others see the problems of spam and already realize a change on the internet; including the fact that the internet changed to a mass medium and that a change of techniques is needed to keep communication on the internet working (Arrison, 2004). However, both groups develop tools to avoid spam. The "ethical discussion" between the two groups of developers (the ones that want to keep privacy while the other ones want to stop spam at any price) take place without taking the users' point of view into account. The following sections describe why it is crucial to take the users' point of view into account.

The spam solutions mentioned in the last section are the most commonly accepted ones approved by scientists and professionals in this area. Other solutions are discussed at the moment and new solutions are presented daily. This upcoming "pros and cons discussion" is a testimony to how complicated this topic is. As examples for such a process I would like to refer to the forums of the Internet Engineering Task Force (IETF, 2007) <http://www.imc.org/ietf-mxcomp/mail-archive/maillist.html#02683>.

2.4.8. Personal Information users have to offer in order to make solutions work

By definition, some solutions against spam need information from the user in order to be able to work. Especially solutions containing an authentication-mechanism imply these possible disadvantages. Users need to offer information to VoIP providers or a central organisation in order to keep the solution working (Cerf, 2005; Arrison, 2004).

The information offered differs from solution to solution. While a provider might argue that the more information offered the better, the fact remains that the information needs to be well chosen. Pay-per-call solutions would just need credit-card information – which then means that the user needs to be registered at a credit card company. Authentication solutions would need name, place and IP-address of the user. These pieces of information would then need to be confirmed by a governmental organisation, a bank institute or any other organization. White and black lists or filter-systems would not need any information, but are very weak. Every solution has its disadvantages; the success of the solutions depends on the users' acceptance. As well the different technique should not foreclose different users. Someone who does not have a credit card shall still have the possibility to use VoIP.

2.5. The myth of users' need for absolute privacy

By using software we often face the question of whether we want to take the correct way or the fastest, easiest, most efficient way. For example when we download files; we should check every file with a virus program, should extract it on another partition than the one our files are saved on etc. But what do we actually do? We just open the file. This usability problem occurs all the time when people are working with the computer. It sometimes occurs because they do not know what they are doing, sometimes because they do not care and sometimes because they simply have too much trust in the computer.

There are a lot of usability studies which show that people are willing to compromise on security or privacy in order to work faster or to work more efficient. Even though, they do

recognize that their action might not be correct, they still do it (Good et al, 2006; Bittner et al, 2005). This problem often occurs because usability is not given. Usability is crucial because even the most secure systems would not be used much if they were too difficult to learn and cumbersome to use. Users would rather choose to bypass it in order to get their work done. Users tend to compromise in order to get a better result. Often, because the systems do not require the usability they should or because the process would be too complicated (Bittner et al, 2005).

However, as already mentioned users are aware of the consequences of their actions and that they are compromising in order to get better results. It was therefore assumed that users would offer information as well in order to get better results. Amazon.com (2007) is an example for this. The more information people offer the better the results become and thus, there is more private information about the users which Amazon can gather. The system is transparent to everyone and there is a trade off between Amazon and the user. Amazon gets better profiles, the user gets better recommendations. Because of that, the user agrees to it.

Shifting the focus now to the research question of this thesis, a similar trade off can be detected; the more information a user offers the better the spam detection becomes. Taking a look at Amazon, as an example, it was imagined that users would cede total privacy in order to avoid spam. The “fact” that users want to be private on the internet at all times might become a myth in the face of today’s problems such as spam. The research shows that the trade off was not accepted by the users in any way, while users would offer private information to some organisations. The analysis in this thesis clarifies this discussion.

3. Methodology

The methodology chapter describes the research in depth and explains the steps which took place during the research. Moreover, it describes the guidelines for the interview in detail and poses the different questions.

3.1. General structure of the research

This thesis analyzes a problem which concerns every-day-users. Therefore, the research puts the main focus on the users' opinions, problems and ideas. During the research users were exposed to questions in a qualitative and a quantitative way. The interviews and questionnaire aimed at finding out the users' point of view regarding VoIP spam, the concerns these users have and whether they are willing to offer anything in order to avoid VoIP spam. The research was subdivided in three steps.

The first step was to send fake spam messages to the target users for the qualitative research. Due to the fact that most users have never experienced VoIP spam voice commercials were created that were used to annoy "VoIP spam inexperienced" users. Thus, an artificial research environment was created (See chapter 3.3.2).

The following second step was to interview the target users. A guideline for the interviews was created, containing the questions that were asked during the interviews (See chapter 3.3.1). These questions analyzed the way people deal with the problem of VoIP spam on the one hand and on the other hand, whether or not people are willing to offer private information to avoid it. A qualitative approach was used in order to get information which describes the concerns and viewpoints in a detailed way.

As the third and last step of the research a survey was created containing more specific questions in order to get quantitative information (See Appendix B). These questions were based on the results of the qualitative interviews (See chapter 3.4). This information was then used to verify the results from the qualitative interviews.

The following chapter 4 explains the result of the described research.

3.2. Target Group

The internet is (still) a modern, relatively young aged medium. This statement is based on some statistics that show that the internet is mostly used by people aged 16 till 24. While the group of users aged 24 to 44 is quite big too, the group of users older than 45 is much smaller (Ottens, 2006; Harmonic, 2006). The reasons for that lie in the fact that the working environment of those people often was not built with the internet, they traditionally do not use the internet or do not want to use computers. Nonetheless, the purpose of this thesis is to determine the target user group of VoIP. While different facts for not using the internet apply to users that are older than 45, some facts for not using VoIP apply to the user group over 30 (Ottens, 2006; Harmonic, 2006). Skype, as an example, is mainly used by users around 25, users over 30 uses Skype by 25% less than users in the mid 20s. Due to that, the main target group, for this research, could be narrowed down to an age of 20 to 30 (Skype-News, 2005).

The main target group certainly is the one described above and the research took place in this target group. Despite this, the low price of VoIP will convince older people of the advantages of the VoIP technology too and the main target group will increase on a long term. But at the same time this new target group will probably be even more annoyed by VoIP spam (because they are not used to spam in any way and because their possibilities and opinions are different). Therefore, their point of view is interesting to take into account for further studies.

To narrow down the target group that was interviewed it can be defined as follows. The users were women or men aged 20 to 30 using computers and/or telephone on a daily basis.

The users were able to handle a mobile phone and/or a computer. The users did not have any knowledge in the computer science background. All target users had experiences with spam in general and have experienced the (dis)advantages of unwanted commercials.

In order to give an idea about the target group, the next chapter describes a person who could have been one interview partner for this research.

3.2.1. Persona as an Example

Linda is a 28 years old employee at a bank in Gothenburg. She studied management at the University of Lund and graduated two years ago with the degree “Master of Business Administration”. She works at the bank between 8 and 10 hours/day. At her job she works a lot with the computer. The software she uses are the email system Outlook, special intern bank software and accounting software, as well as the whole MS Office package. Besides working on the computer she communicates a lot with her colleagues via telephone, intranet or in meetings.

During the evening and weekends she usually stays at home and watches movies or talks to friends; in person or via telephone. Linda is a very communicative person and it is possible to reach her all the time (except during work time). Due to the fact that she talks a lot on the phone in her leisure time she is always interested in having the cheapest telephone operator. Therefore, she checks the cheapest prices for telephone and mobile phone quite often. She switched phone operators twice over the last three years.

Even though she is quite experienced in working with a computer (due to her job) she does not have a computer at home and therefore does not have the opportunity to use any internet services. Even though she has a private email address she usually checks it on her friend’s computer. The same goes for her surfing the net and gathering information on the internet.

3.3. Qualitative Research

During the qualitative research target users were questioned about their point of view in regard to the research questions. The questions were kept open to give the users the opportunity to express their thoughts and to examine (un)certain behaviours of the users. It was important as well to get an overall picture of the whole situation of every user, instead of just getting straight answers; on the one hand to see how questions are interpreted and to ask broader questions and on the other hand, to get more valuable answers.

In order to draw up the guideline and to examine whether the results can be used the questions were tested on one user before it was used for researches on a broader base. Section 3.3.2 describes the commercial prototype and the way it was used, section 3.3.3 describes how and when the research took place and describes in detail the field of application.

3.3.1. Guidelines for the interviews

This section describes all the questions the guidelines for the qualitative research contained. The aim was to answer the general research questions of this thesis; “Are people willing to offer private information in order to avoid telephone-spam? What kind of information are they willing to offer?” and additionally “Are people even willing to pay for it?” Every question will be presented and evaluated to show how and why the questions are important in relation to the research questions of the thesis.

1. Do you receive unwanted-telephone-calls; How many a week?
 - None
 - 1-5 calls a week

- 5-10 calls a week
- More than 10 calls a week

2. When do you receive unwanted-telephone-calls?

- During Work/School
- During Free time
- During Night

The first questions are more or less questions used for checking whether and when people receive spam calls. The questions intend to clarify if people have the necessary background to be able to answer the following questions. The second question shall already give information about the factor of annoyance while it is obvious that a call during the night might be more annoying than a call during work time.

3. How did you react on unwanted telephone calls?

- Listen to the message
- Hung up
- Try to answer
- Did not answer the telephone next time
-
- Other _____

4. What kind of thoughts did you have after the call (that was fun, hope they won't call again...)?

5. Was your daily life disturbed by such calls? In what way?

7. Have you tried to get rid of unwanted-telephone-calls? What did you try to do?

These questions shall underline the users' reaction to the calls and shall already give a feedback on the users' factor of annoyance. When users are very annoyed by such calls it may be an indicator for the peoples' willingness to offer information in order to just stop the unwanted calls.

While question 3 asks about the direct (re)action, the questions 4-6 encompass a broader range, they ask about the influence of the calls to the users' life. If the calls have an influence on the users' life it is likely that a user wants to get rid of the calls. Later questions in combination with this will analyze whether the factor of annoyance has something to do with the offer of information; the factor of annoyance stimulates the users' willingness to offer information to organisations, companies etc.

6. Did you have any costs by receiving unwanted-telephone-calls?

- Voice mail (Costs for calling the voice mail)
- Cost for roaming (Receiving calls outside the country)
- Forwarding costs
-
- Other _____

People surely do not think about the fact that they just lost money by calling the voice mail and that they have just received five spam messages. They probably do not think about it when they are on vacation at the beach. But when facing the question, they will recognize that they have actually lost money. This question intended to question if they are willing to pay for spam.

8. Within a week, how many unwanted-telephone-calls would you accept?

- None
- 1-5
- 5-10
- I do not care

This is a rule- out question for filtering techniques. If people actually do not accept any spam mail the technique of filtering VoIP spam calls becomes questionable due to the lack of protection.

9. Would you pay a monthly amount to get rid of unwanted-telephone-calls? How much? (Take into account to receive spam on the voice mail or in another country)

- Less than 10 SEK a month
- 10-50 SEK a month
- More than 50 SEK, as long as I get rid of it

With Question 9 the user is faced with first facts. This question proves the ability to pay for a solution for VoIP spam and connects directly to payment-solutions.

10. Would you give up anonymity to avoid unwanted-telephone-calls? To whom? Who may save your personal information to avoid unwanted-telephone-calls? Fill in following table:

	Government	Service Operator (Telia, T-Mobile, Skype, Sippgate)	Companies / Systems (OpenID, Microsoft, Google)	Organisations (W3C, ICANN, NIX)	No one
Name					
Social security number					
Residence information					
Telephone records					
Credit Card Information					
Bank account numbers					
internet history					
IP address					
date, time and duration of your calls					

In connection to the given solutions the table in question 10 supports the gathering process of facts. The users' answers to the different rows in the table make it easy to draw a direct connection between the different solutions and the users' point of view. As well a reconnection to further questions it is possible to see how the users' point of view is connected to the factor of annoyance by spam calls.

If you would receive the same amount of unwanted-telephone-calls on a long term (a year) as you received during the last week.

11. Do you think that unwanted-telephone-calls would influence your daily life? How? Would you use your telephone differently than you do today?

These questions aim at taking a look into the (near) future and to get an idea about how the users' behaviour may change. Because the users knew that the spam attacks would stop after a while they may not have changed their behaviour the way they would have when confronted with a long term spam attack.

12. From your point of view: who should develop unwanted-telephone-calls solutions and why?

This question is not connected to the different solution in the first place but users may have different opinions about who shall develop solutions.

13. Do you use Skype or any SIP telephone?

- Yes, often
- Sometimes
- No, never

14. Do you buy on the internet (Amazon, CDon, ebay)?

- Yes, often
- Sometimes
- No, never

13 and 14 are checking questions. They shall show the extent of users' understanding of the internet and whether they already offer information without knowing about it. By being registered, e.g. to Amazon.com (2007), it is obvious that users offer bank account information to such company. Users probably do not want to offer information to different providers but a conflict might occur at this point.

15. Sex

- Male
- Female

16. How old are you?

- 15-20
- 20-30
- 30-40
- 40+

15 and 16 are general research questions to order establish target groups.

3.3.2. "Voice Commercial" – prototype

As stated in the chapter above, many users did not have any experience with telephone spam; and consequently they did not have any experience with VoIP spam. To introduce these users to the research and in order to ask them questions, it was important to create an environment which presents the problem to such users. They needed to experience how VoIP spam would influence their daily life and their relationship to the medium telephone. Therefore they were confronted with fake spam calls. This section explains how these fake spam calls looked like.

First of all, it is important to say that I used the technology of VoIP telephony to send fake spam calls to the test users' telephones. The test users agreed before to be part of the research but did not know what the research was about. They did not have any idea that the spam calls they received were fake spam calls that were connected to the research. Surely, it could be discussed if this method of sending spam messages without the knowledge of the user is ethical. But in order to build a realistic research environment and due to the fact that I was able to intervene (by listening to the users' reaction) I chose this way of research. As well the

amount of was a small one, while doing a wider research it would surely be important to have a discussion about the ethical standpoint of the research.

As a rule, it is even quite easy for a novice to spam people who have a normal telephone number. As a player-device I connected a MP3 player with the voice-in connector from a computer and randomly called the test users via a softphone. The moment they answered, the voice commercial was played. The softphone application used for the process was a SIP telephone from the company Sipgate (Sipgate, 2007). The users only had the opportunity to listen to the prototype while I had the opportunity to listen to the users and coordinate the commercial at the same time. In doing so, it was possible to intervene when the users' reaction became too harsh. In fact I was forced to stop the research before I was able to send more than ten fake spam calls because of the harsh reactions of all users (See section 4.3.1 for more information). By obtaining the user the aim was not to gather research data than only to control the calling process.

The research contained three different commercials that were repeated over and over again. One spam commercial was used to reach a receiver more than once, because spammers try to send as many of the same spam emails as possible at the same time to increase the plausibility. It is quite obvious that the same way of sending will be used for VoIP spam too. As a matter of fact, repeated messages are much more annoying than different commercials.

Besides the technical part (see section 2.3) the content of the spam mail needs to be taken into account as well. Serious companies will not use the technique due to prohibition. Thus, the brochure ware will be products such as pharmacy, erotic and other similar products; such products email spam messages use to promote. The commercials I recorded contained content taken from these areas. The texts are published in the Appendix C.

3.3.3. Field of application

When using a voice commercial, it is important to define “when” and “how” it is used. It is important to define the when and how people would face VoIP spam as well as how much VoIP spam they would receive in a realistic way.

Transferring the number from email spam to VoIP spam would surely be wrong, due to different facts: It is much more expensive to send VoIP spam than to send email spam; VoIP spam needs to be more personalized than email spam; VoIP spam to one address cannot be sent in one batch but needs to be sent successively; etc. In addition to that, it is important to take into account that even VoIP spam filters will detect a huge amount of spam which will then be erased before it is received.

But there are some facts that can be transferred and can help to build up an algorithm how to ‘spam’ the target user group. Even though email spam filters seem to be quite efficient they let some emails pass every day. It is especially when a new technique is used that some filters leak and let huge amounts of spam get through to the inboxes of the receivers. A very advanced and popular mechanism to distinguish illegitimate spam email from legitimate email is Bayesian filtering.

Bayesian filters, considered the most advanced form of content-based filtering, employ the laws of mathematical probability to determine which messages are legitimate and which are spam. (Satterfield, 2006)

It is based on statistical filtering and this is also why especially new types of emails get through to the receiver. Not taking the simultaneous spam mails into account one to three percent of all spam emails end up in an inbox. Even though it is possible to extract a number between five and fifteen spam calls that could get through to the recipient, the ordinary poll-taker telemarketing calls are not taken into account yet. The problem of telemarketing calls

already occurs today and aggrieved parties already report about five to 15 calls a day; during day and night (Antispam, 2007). Combining telemarketing and potential VoIP spam calls a number between 20 and 30 a day comes up. This number certainly is huge but still a quite realistic one.

In order to describe a scenario that introduces the inexperienced to the problem but does not influence their behaviour in daily communication and life too much, a number of five calls in 24 hours were used to give the target user an idea. Because the repetition of spam makes the situation even worse, the fake spam attack took place for 72 hours and contained 15 calls. This mirrors 50% to 100% of all calls a target user received in 72 hours and was therefore acceptable and visualized the problem of spam on the phone quite well at the same time. This derivation took place in relation to this research and approximated the number of calls.

The fake spam calls were only sent between 7am and 11pm in order to aware the users' privacy.

An important factor for confronting users with spam calls was that such calls become a nuisance after a short time. Due to the fact that some users never had experienced such calls they were interested in the content of the call (for personal amusement) and did not even realize the actual problem, in the beginning. Carrying out the research, it was therefore important that the content of the fake spam calls became uninteresting for the target users. The aim was to make the messages as little entertaining as possible due to the short test period. This aim was reached when looking at the users' reactions regarding the fake spam calls (See chapter 4).

3.4. Quantitative research

The qualitative research examined the viewpoints of the different users in a detailed and profound way. Based on the information that was extracted from the qualitative research a questionnaire was drawn up in order to research the topic quantitatively. When drawing up the quantitative questionnaire it was important to get Boolean answers, Yes- or No answers, to such questions. That includes that the questions were simple, clear and did not have a double meaning. The purpose of the quantitative research, in addition to a qualitative one, was to verify the results of the qualitative research on a broad basis. Responses from many users verified/falsified the given results and clarified that the research was necessary and useful.

The quantitative questionnaire is published in the Appendix B.

4. Results / Discussion

4.1. Overview

The research showed many expected results but also brought some interesting surprises to light. To give an example, the users' reactions to the fake-spam-calls were so extreme that I had to stop the experiment after six to ten calls. Already after the third call one person started to call the operator in order to stop the calls in any way. Moreover, they adopted different telephone behaviour as well, e.g. they did not answer calls or put down the phone after the first few seconds.

The complementary quantitative research, that took place in order to support the results of the qualitative one, confirmed the results that came up in the quantitative research (The questionnaire is published in the Appendix B).

4.2. Description of test users

In order to give an idea about the test users who took part in the research this section shall introduce the different user groups.

In order to receive results for the qualitative research the goal was to fit the target group made up of users aged 20 to 30 (See section 3.2). Five test users between 23 and 28 were interviewed. Three of the users were from Sweden, two users were from Germany. Three of the five users were male. Only one person had experiences with telephone spam before, the other ones were confronted with telephone spam for the first time during this experiment. All users use the internet for communication purposes and some of them even trade on the internet once in a while. Most of the users use Skype (2007) as a communication tool and therefore fit the target group of users who search for less expensive means of communication very well. All of them were at least experienced in talking on Skype or SIP.

The quantitative research took place on the German website www.antispam.de (Antispam, 2007). It was based on 24 (anonymous) persons who filled out the questionnaire online. All of them had had experienced telephone spam. Ca. 85% of them receive between one and ten calls a month, while most of those users receive less than five calls a month. Surprisingly, more than half of all users never used a Skype or SIP-telephone and 30% only use it sometimes. Half of them buy online often and the other ones sometimes. The questionnaire took place under the section telephone spam. The website represents a forum for spam "victims" who exchange information about all sorts of spam, problem solving, etc.

4.3. Analysis of research data

The following sections will present the results of the research and the answers of the different users. The analyses of the qualitative research will be described in the first section and the analysis of the quantitative research will be described in the second section. The following section then relates the research-analysis to the different VoIP spam solutions in order to evaluate the most accepted solution in relation to the research. The main weaknesses of this research could have been the questionnaire and the discussion with the people taking part in the research. The questionnaire might have included ambiguous questions which might therefore have been difficult to answer. If this were the case, test users might have been irritated by a question and might not have been able to answer it. Another probable scenario was that they answered the question in a way they did not intend to answer it. These actions would not only have altered the result but they would probably have had a deep impact on the research as a whole. Fortunately different indicators show that the scenario did not become

true. The most important indicator is the users' feedback on the questionnaire that shows that they understood the questions and were willing to discuss different options regarding one question.

4.3.1. Analysis of qualitative research

The qualitative research brought forth many results. All users stated that their daily life was disturbed by spam calls. That became especially clear by the fact that I was forced to stop sending fake spam messages because the users' reaction to the messages was very harsh. The test users were annoyed mostly by the fact that the calls interrupted their activities they were doing in that moment to answer the phone. A description about the people that were interviewed is found in chapter 4.2.

	1. What kind of thoughts did you have after the call? (Question 4 in interview - guidelines)		4. Do you think that unwanted-telephone-calls would influence your daily life? How? (Question 11 in interview - guidelines)
User 1	Not again	User 1	Yes, a lot, would only answer the phone when a caller-ID is shown
User 2	What the f***, calling and annoying me while I am not interested in their messages.	User 2	Yes, one would be disturbed during important meetings etc. Additionally, one has an awkward feeling if the phone rings all the time.
User 3	Became very angry	User 3	Absolutely, I would have contacted the telephone operator and complained about it. As well I probably would have changed my number.
User 4+5	Just annoying	User 4+5	A lot. In different ways.
	2. Was your daily life disturbed by such calls? In what way? (Question 5 in interview - guidelines)		5. From your point of view: who should develop unwanted-telephone-calls solutions and why? (Question 12 in interview - guidelines)
User 1	Becoming very unfocused on what I was doing and probably missed important calls because I was not answering the phone any more	User 1	Telephone operator (no reason)
User 2	Sometimes I was woken up by such calls	User 2	Telephone operator because they want to have happy customers.
User 3	Felt a bit awkward	User 3	Someone who has a solution for the problem
User 4	It was just annoying	User 4+5	Probably telephone operator or governmental organisation?
User 5	Daily life always is disturbed when receiving calls.		
	3. Have you tried to get rid of unwanted-telephone-calls? (Question 7 in interview - guidelines)		
User 1-3	No, nothing		
User 4	Called my telephone operator to act		
User 5	Called police and telephone operator. Informed ourselves about caller-ID		

Table 4.1: Users' reactions on spam calls; answers from the qualitative research

All users were asked to describe their feelings and all of them described their feelings as "really annoyed" up to "very angry". Their verbal reactions were quite harsh and confirm the fact that the users were not only annoyed but actually really disturbed by the spam calls. It confirms the fact that spam calls actually annoy its receivers in a more critical way than common email spam. To describe users' behaviour in relation to the spam calls the following parts will give an insight.

At the beginning of the fake spam calls all test users listened to the message, but after the second/third time they all started to just hang up. They already became very annoyed after only a couple of calls. Probably their reaction would have been less aggressive if not a machine than a person would have been on the other end of the line and would have talked to the person instead of hanging up the phone directly; even though the users would still have been disturbed in their daily life. In fact all users announced that they would not accept any spam calls at all for their daily life, what confirms the high level of annoyance, independent from the fact if a machine or a human is the dialog partner.

Even when the users were so annoyed only two of them actually tried to take action against telephone spam. Both of them called the operator while one person even contacted the police (See table 4.1, section 3). The reaction of those two users already shows a trend that users try to solve the problem by contacting the operator or a governmental organisation. They search for a solution by contacting the authorities that are in direct connection with the phone and they seem to trust them while holding them responsible at the same time.

A confirmation to this argument of trust and responsibility was given by the answer to the question whether people “would give up their anonymity in order to avoid unwanted-telephone-calls”. All users agreed they would hand out all information to the government, while only being inclined to disclose name, residence information and social security number to the telephone operator. No user would offer more information than name and information of residence to private companies. Users were (surprisingly) suspicious of handing out information about themselves even though they were aware of the fact that spam influences their daily life to a great extent. The trade-off between handing out personal information and therefore receiving less spam was seen as doubtful. They more or less only wanted the administrative organisations such as governmental organisations to receive personal information in order to solve the given problem. This assumption was confirmed by the answer to the question “who should develop unwanted telephone call solutions and why” (See table 4.3). Except for one user all users made the telephone operators or the government responsible for the problem. One user cited as a reason that these “operators should provide the service to please their customers.”

A really unexpected result was shown in an answer to the question whether or not users would pay a monthly amount to avoid unwanted telephone calls. Only two users would agree to paying 10 to 50 SEK to get rid of spam, the other ones did not want to pay money at all. This seems to stem from the fact that the phone calls as such are unwanted and that users do neither hold themselves responsible for the calls nor hold themselves liable (by paying a monthly amount) in order to avoid those calls (See table 4.3).

4.3.2. Answers to quantitative research in comparison

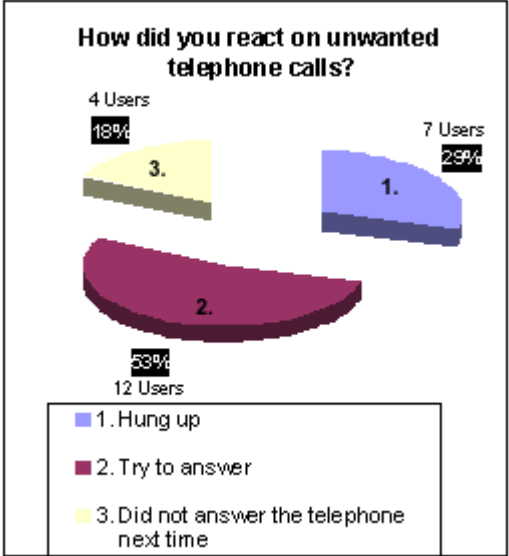
The quantitative research confirmed the results which were received by the qualitative research. The most adequate answer results from the question “if people would pay to avoid spam and how much they would pay”. 24 persons were interviewed on the German website www.antispam.de (Antispam, 2007); a description of the persons is given in section 4.2. The figures 4.2 and 4.3 show the results from the quantitative research. The questionnaire was translated from English to German in order avoid misunderstandings. The questionnaire is published in the Appendix B.

Except for three users, ca 13%, no one of the target users would pay anything or if so, less than 10 SEK for a solution against spam. This confirms the fact that private users in general are not willing to pay for anything they do not want to have. One user even named monthly amounts of “protection money” because then these companies would receive money for stopping the spam call (See table 4.3, answer user 2).

Only one of the test users, ca. 4%, was willing to pay more than 200 SEK to avoid spam. He was actually willing to pay – as long as he would avoid spam. This may result from the factor of annoyance.

Another point of view the users had in common on their private information. More than 90% of all users would not offer credit-card-numbers and bank-account-numbers to others, while more than 80% would not offer IP addresses to anyone. While most of the questioned users would offer name, address and internet-history to the government only five users, ca 23%, would offer the same information to telephone operators and only two users, ca. 9%, to private companies.

- 1. How did you react to unwanted telephone calls?**
- 12 Users I ask the caller to delete my data from their database.
 - 4 Users Be unfriendly and did not answer next time
 - 7 Users Put the receiver next to the phone and wait or directly hung up



- 2. Have you tried to get rid of unwanted-telephone-calls? What did you try to do?**
- 1 User Contacted legal authorities
 - 9 Users Do not answer calls from unidentified callers
 - 1 User Contacted the police
 - 9 Users No actions

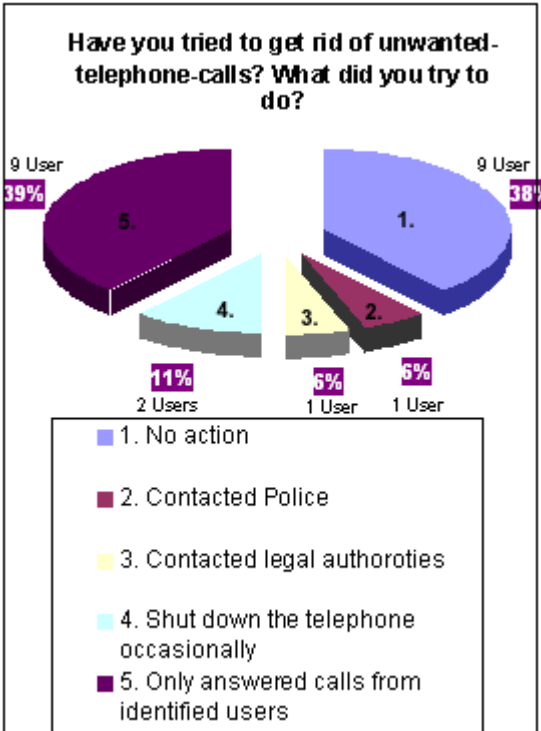


Table 4.2: Users’ actions on spam calls; data from the quantitative research

These results confirm the results from the qualitative research and show what kind of organisations user think of as trusting. Trusted organisations are governmental organisations

and telephone operators. Private companies are kept out of this. Moreover, the users think of these two parties as responsible for developing solutions against spam. More than half, 52%, of all users think of the government as responsible, one third, 33%, thinks of telephone operators and only one fifth, 20%, of private companies. Still more than 40% agree that first of all it is important to develop a solution, they did not care who shall develop it.

The way people experience telephone spam was similar to the qualitative research as well. Nearly 80% said their daily life was disturbed by telephone spam. One third even said that their daily life was permanently disturbed by telephone spam. Only three users, ca. 16%, said their daily life was not disturbed by telephone spam at all.

The answers to the question what actions people took in order to avoid telephone spam and how they reacted to the telephone to spam calls differed more widely. One third, ca. 30%, did not take any action against telephone spam while another third, ca. 30%, started to answer calls with caller-ID only. Two users put down their telephone occasionally. One user even called the police and another one called the telephone operator. Some users added the information (to the questionnaire) that they even send a written warning or a caution to the companies as well as to the federal telephone-network agency.

Comments on the problem of unwanted telephone calls

- User 1 I have received unwanted calls since I changed the operator; I was before a Telekom member and I changed to Arcor. Until now the choice of the operator was the expenses; next time I will choose the operator by its annoyance. But how to know this in advance?
- User 2 From the legal point of view it is obvious that no company is allowed to send spam emails. Why should I pay? I probably pay the companies that call me to stop calling. Protection money?
- User 3 It is important to get a clear legal constellation. In that way things such as Black lists or Spam filters do not need to be activated.

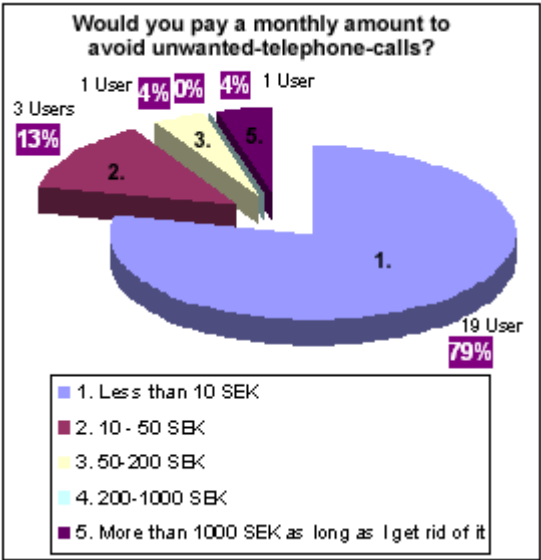
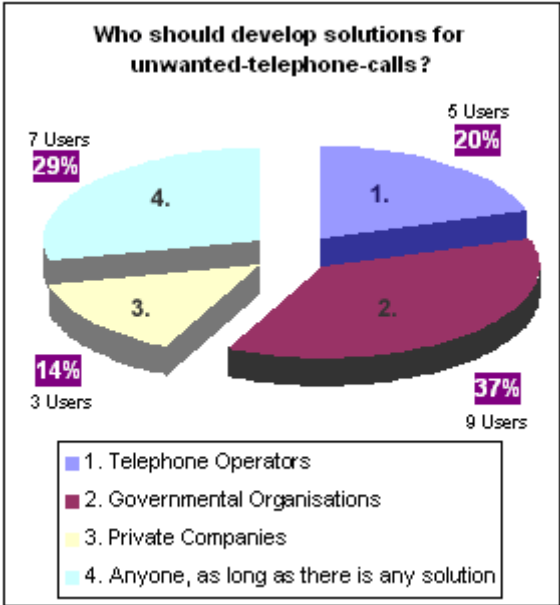


Table 4.3: Comments of users; data from the quantitative research

The way people reacted to the calls differed from person to person. Ca 40% tried to talk to the person that was calling in order to express the annoyance and to try to make them stop calling. Every fifth user, ca 20%, just hung up and ca. 13% did not answer the telephone the next time (See table 4.2). Some users added the same reactions as before; they tried to hold the caller liable for consulting the federal telephone-network agency. All in all, the results from the qualitative research were confirmed by the quantitative research. Only when answering questions on users' behaviour did the answers differ, which is an indicator for the different experiences in the field of telecommunication and knowledge about their rights on what call centres are allowed, or not allowed, to do.

4.4. VoIP spam psychological component

VoIP spam influences users' life in different ways. One component is that it is annoying to answer the phone and it takes time to talk to someone. But another component that influences the user even more is the psychological one. All users, including men, described that they felt really annoyed by the calls. Calls imply an importance, they are seen as urgent. Therefore people hurry to answer the phone and thus they get even more annoyed while answering the phone and it is just commercial at the other end of the line.

Especially women stated that they felt unwell answering the phone to someone unknown at the other end of the line. When the phone was ringing during the night they preferred a man to answer the phone because they felt much safer then. But men as well described the fact that someone unknown was calling as "unwell". The information was provided by the users in addition to the questionnaire.

The reason for users feeling unwell may be that users felt as if they were being watched in some way. And the recurring question seemed to be "how did they get my number" and "who is actually calling." The unknown components seem to influence the user the most. Users would probably get less afraid when receiving more telephone spam and getting used to it, but it still is psychologically stressful for the user in any case.

4.5. Analysis of research results in relation to VoIP spam solutions

In this section the answers of the test users are seen in relation to the different VoIP spam solutions. The users' point of view is important for developing spam solutions in order for the different solutions to be widely accepted.

The first VoIP spam solution I would like to discuss is the **pay-per-call** solution that was introduced earlier by Arrison (2004). The research showed that people are not willing to pay any amount of money to avoid telephone spam. Even when they stated that they were really annoyed by the unwanted calls they did not agree to pay for "not receiving spam". The acceptance to pay for a service that is not really needed yet seemed absurd to the users. But users' answers to the question whether they would use the phone differently when receiving spam on a long term basis, show indeed that people actually would stop using the phone or switch it off. Many people cannot switch off their phone, mostly for business reasons. Therefore the pay-per-call solution could indeed find its target group. But it could not be used in the way Arrison (2004) described, on a mass market for end users, that would probably be a solution more or less for some groups or companies that have a high need to avoid spam. It would be necessary to adjust the technique to its new target group.

Other solutions that seem to be useful but do not provide the key to the problem are the techniques of "**Filtering at the receiving end**" and "**Turing tests**". The techniques were described in the theoretical foundation by Cerf 2005 (Filtering at the receiving end) and Gburzynski et al, 2004 respective Rosenberg et al, 2004 (Turing tests). The test users indicated that they are not willing to receive any spam calls. Users would probably accept one or two calls as explained in the theoretical foundation, the technique of filtering would let some calls slip through. Filtering such calls is quite difficult. While emails are much easier to examine, calls are due to the fact that they are synchronous, much more complicated to examine. The test users were already annoyed to a great extent by only five to ten spam calls, leakage in a spam filter would let much more spam through to the receiver. Users would become even more annoyed when already having activated a filter and still receiving a lot of VoIP spam calls.

A similar problem occurs in the **Turing tests**. Even though this solution blocks out computers that ring automatically it would not block out VoIP spam. It just makes sure that a human need to sit in front of a computer and fulfils the Turing-requirements; afterwards the machine could take over. Taking into account that VoIP spam could be sent from all over the

world; cheap human resources could be used to fulfil the requirements by guaranteeing low prices for every call. As well some programs are already able to detect Turing tests such as CAPTCHAs (Mori et al, 2007).

A more promising solution seems to be the **authentication** solution (Cerf, 2005). Users' restriction lies in the fact that the authentication needs to be resolved by the government and not by any company. The test users were very afraid to disclose their personal information; even when they were very annoyed by the telephone spam. Even though most of the users buy their train ticket or a CD online they are very conservative when it comes to handing any information to third parties. In order to get solution which is accepted by most people it would have to be announced by the government in order to eliminate the users' doubts. The problem in this short-term-business surely is the complicated bureaucracy while introducing a solution against spam. But a private company would not have a strong impact on users.

Other trustworthy organisations seem to be mobile phone operators. A general point of view of the test users was that the operators or governmental organisations shall develop VoIP spam solutions. The test users hold them responsible for proper solutions and they trust them when it comes to their personal information as well. The prerequisites for a solution, however, are not good because telephone operators would need to work together and form a union against spammers; while spammer could be respected clients of the different operators. To overcome the spam problem, telephone operators would probably need to dismiss their own clients; the spam senders.

If VoIP providers and the government built a union against spam by a regulation or providers' - "spam free certificate" users would trust them with their personal information. This would be a good chance for developing strong solutions against spam.

4.6. Spam solutions in relation to the research

In the following sections I will present the most realistic- as well as the most promising spam solutions. These chapters are based on the results of the research but are influenced by my personal opinion and my experiences in the respective areas.

The most realistic solution is based on the research and facts while the afterwards following chapter is more based on a case and does not reflect facts but rather an "optimistic point of view".

4.6.1. Most realistic VoIP spam solution

In the section above I have already mentioned a solution which could solve the solution by having a control mechanism between the government and the telephone operators. However, especially the bureaucracy of governmental organisation would destroy any cooperation plans. It seems quite probable that it would take too much time and money to create a solution that would fit the given expectations. Other companies would conquer the market with functioning solutions a long time before the government or a telephone operator would present a functioning solution. Users would be forced to choose a solution that actually does not conform to their ideals in any way. Taking a look at today's VoIP market, Skype (2007), as the leading operator, already has harsh restrictions for authentication.

My hypothesis for a VoIP spam solution is that users will not act according to their values but would rather switch to the operator which has the best VoIP solution rather than to wait for any operator-comprehensive solution. Especially the fact that users are very annoyed by telephone spam and the fact that users do not want to pay for spam detection points to a solution in which the operator uses the product-wide-authentication as a spam detector. Skype already pushes forward such a solution and seems to detect spam successfully because there is only very few information available which records VoIP spam attacks on Skype.

I think that the small SIP-providers can only solve the problem of VoIP spam by working together with each other and trying to push the government for quick restriction. In that way, they could fulfil users' interests and solve the problem the same way. The government certifies the different providers. Those providers which fulfil the restrictions become certified. The certified providers allow communication through each other without any restrictions. Calls from providers that are not certified do not get through to the "network of certified providers". If a spam call does occur inside this network it can be traced back to the provider. The provider is responsible for making sure that the caller is made liable for the spam calls. If a provider does not meet his responsibilities he is made partly liable for the damage of the spam calls and is kicked out of the network.

The advantages are that providers are forced to get this certificate in order to be able to survive in a competitive market like the Swedish or German one. Moreover users can choose the provider by the certificate and can in that way make sure that they are in the safe zone.

The disadvantages are that providers need to save users' private data in order to make users liable for spam calls. A cooperation of SIP-providers, including Skype, and the government is a realistic scenario and would keep out telephone spam. See figure 4.4 to get an impression of the solution.

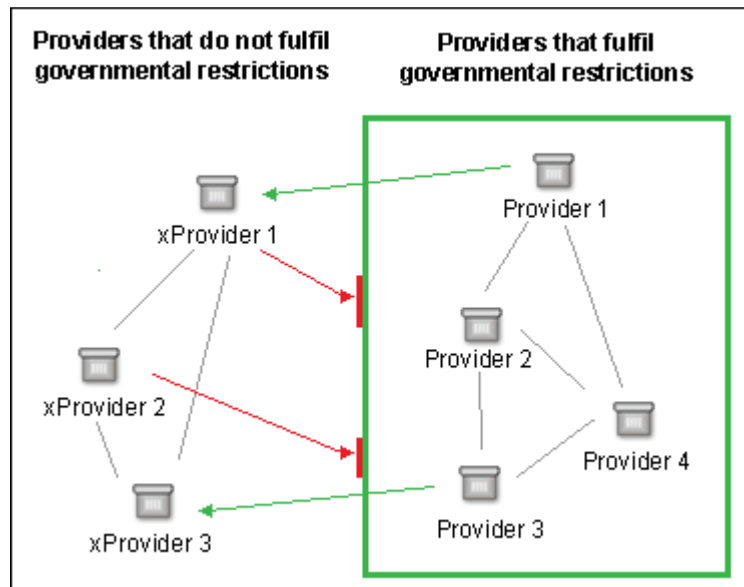


Figure 4.4: Most realistic spam solution

4.6.2. Most promising VoIP spam solution

There are a lot of promising solutions that could solve the problem of VoIP spam and could be accepted. This chapter shall present the most promising solution in relation to the research results.

I would like to start the discussion by taking the "pay per call" solution into account that was former introduced by Arrison (2004). Due to different facts, it seems that this solution would change the whole spam problem to a win situation for end users. While users can choose how expensive it is to contact them, provider would contact users not randomly but more specifically. The whole telephone-marketing market would have to appear more respectable and by that more understandable for the end-users. And, even better, users would get paid for every call. The aggrieved party would become the beneficiary party by making money through spam calls. It should be researched if a solution such as a "reverse charge call" could be realized; adapted to the given topic. People who do not offer personal information, and cannot be traced, have no other option but to pay for a call. However, this seems to be difficult to realize. The way Arrison (2004) described the pay-per-call solution would have difficulties in becoming accepted since a user has to offer lots of information. A more specific, personalized solution such as reverse charge calls would probably become accepted much quicker.

In addition to that, a very promising solution would be to analyse the telephone habits and records of private persons. None of the described approaches takes the individual's telephone habits into account but always counts all telephone users as one. A more personalized solution

would make it possible for every user to set filtering restrictions. For this, it would be important to analyse telephone habits of individuals. In a lot of cases they will show that most calls are done inside the borders of the country the telephone is placed. By taking into account that spamming is not allowed in the European Union, it becomes clear that no caller with the same country-ID as most of callers would be able to send spam-messages. Therefore, all callers with the selected country-ID are allowed to get through. Today, it is only possible to differentiate between an unknown user, calling from anywhere, and a known user, showing his caller-ID. Telephone operators and the government would need to find a way to change an unknown user to an unknown-fromAnExemplatoryCountry-ID.

So, what to do with the callers that do not have the same country code? Those callers are important too but they are much more complicated to analyse. By working with “Black-lists” and “White-lists”, letting only country codes through, callers who call from another country are blocked. Here it is important to research who is calling and why someone is calling. By receiving only calls from well known persons it would be possible to add those numbers to the white list and block all other numbers with no problem at all (See xCaller1 in Figure 4.5). Even when there are some calls from unknown persons it would be possible to let only those callers through which identify themselves by showing the caller-ID. Those who do not show their caller-ID receive a message that asks to activate a caller-ID. In that case, every caller has a fair chance to contact a user who in turn has a good chance to get rid of spam. Different users are already programming their digital telephone-boxes that way. They forward users with unknown numbers to a voice mail that tells them to leave a message or to activate a caller-ID. Not surprisingly, they state that their solutions work quite well for their purposes (Antispam Forum, 2007). It seems that not one solution is the best one but rather the combination of different solutions.

The presented way may be a good way for private persons. But that is not good enough for companies or private persons who often receive calls from other countries. Companies often have the problem that they receive calls from parties they do not know; but on the other hand they have the advantage of financial power. Different approaches are possible to free companies of spam. As private users they would be able to differ between country-IDs and caller-IDs. For solving the problem of differing between VoIP spam and common VoIP calls from other countries, spam filters could be used. In this case, these spam filters combined with a Turing test could be used. In that way, at least a huge amount of spam could be filtered. But receiving such spam would actually not influence the receiver’s habits much. This is because users in companies respond to their telephone directly and are used to their phone ringing all the time. They do not stop to eat, wake up during night or leave their sofa because of a call but rather sit next to the phone, expecting calls. As well they do not become important to the calls they receive during work than they leave the office after work and do actually not care if there are any other calls.

It will be hard to put into effect to get every user free of VoIP spam but it would nevertheless be possible by combining different VoIP spam solutions in order to get to a VoIP

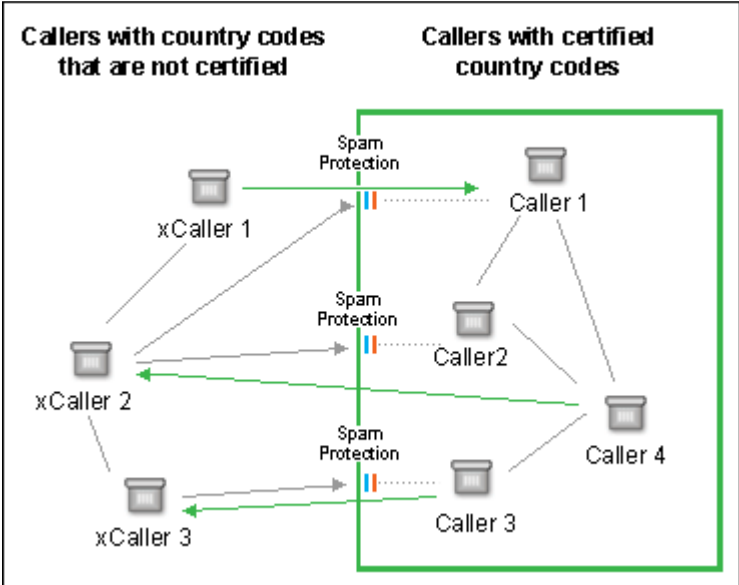


Figure 4.5: Most promising spam solution

spam free society. It is important that the government uses its power to release harder restrictions against spam and work together with telephone operators. The presented solutions can only be put into effect if the government and the telephone operators work on the solutions together as well as using the users' telephone behaviour to stop VoIP calls. It is important to identify and analyze the incoming calls at its roots to find a proper solution. Users can protect themselves better than if someone else is making assumptions about a wide range of users. For example a user can decide for himself if a caller without caller ID is allowed to call him or not.

From my point of view, VoIP spam solutions should therefore become more personalized. Only the user himself can decide whether a call is important or not. The user should decide whether he actually needs to receive calls during the night at all, or whether he needs to receive calls from countries outside the EU. The user should have the possibility to make a decision himself about receiving calls or not and by that change the settings on a filter himself (see figure 4.5). By localizing the own "caller groups" and leaving out the unimportant user groups, it becomes very difficult for any system to be included into these groups of callers.

The protection can be extended the way the user wants to; therefore a payment solution such as "reverse charge call" could be added as well. It could be just a short notification that the user needs to identify himself or a filter or any other solution. It does not matter what kind of solution is used as spam protection. Calls from certified users from other countries are allowed to pass the filter as long as the user allows them to pass.

Advantages of this solution are that every user has the possibility to set the spam protection according to his needs, thus customized spam solution for every user. The solution would make it possible to add nearly every of the given approaches.

See figure 4.5 to get an idea about the solution.

5. Summary and Conclusion

After a research is carried out this chapter shall conclude the research and give an idea about possible further researches.

5.1. Validity / Reliability

This section shall provide a reflection on the research and discuss its validity as well as its reliability (Andersen, 1998).

First of all I will analyze whether the research was a valid one, and whether the results have a true value. The fact that some unexpected reactions occurred, shows that the users were able to answer freely and thus provide some unexpected answers. In addition to that, the users were able to understand the questions and add information they were not asked for. They were interested in the field of research and wanted to know how urgent the topic is and they even showed willingness to answer further questions if needed. Furthermore, I was able to connect the results to the different VoIP spam solutions and to come up with a result and a recommendation for a system which reflects the validity of the research. Even though I did not recommend any system in particular; clear insight of the user's point of view was gained. The most important research facts that users are not willing to offer private information to companies or to pay a fee to avoid spam were confirmed by four of five users of the qualitative research and more than 80% of users from the quantitative research. These high numbers show the reliability of the research. Moreover, most pieces of the further information which was extracted by the research show similar results and become significant by that.

This paper was written as a bachelor thesis at the Växjö University / Sweden. Because of extremely limited research possibilities by human resources, time and money, the research has to be viewed as an approach to how the problem could be researched and it gives an overview about problems, solutions and reactions regarding the topic. Even though, good results were discovered that can be used in order to argue for good or bad spam solutions. It needs to be taken into account that the two presented solutions in chapter 4.6 were built on the gathered research data. These solutions present not the most profound solution than two possible solutions. But, by using the research data the solutions were approved and fit the requirements that can be stated by the research.

Taking into account the results, it is important to analyze whether the research was a reliable one, too. The topic of VoIP spam is still vague, because VoIP spam does actually not exist today. Therefore the question of how to reflect on this problem in the correct way arises. To illustrate the research area, users faced VoIP spam in an artificial way and were then interviewed afterwards. The users' lack of experience in the area of VoIP and the fact that the research area needed to be re-enacted made the research quite difficult. It is always better to research a problem which actually does exist and does not need to be explained in an abstract way. Nevertheless, the chosen method of annoying the test users with fake spam calls created the impression of a reality-scenario and was therefore highly valuable.

The test users from the qualitative interviews were chosen by age and experience with mobile phones and computers. All interviewed persons were students or former students, which leads to the question if there was a selection of users. Surely the group of higher educated users may influence the result by the way the users react to the fake spam calls but they can be seen as target users because they are curious about new ways of communication. Because VoIP is such a new technique and because it still requires certain skills a higher educated group of test users describes the target group well. As well the results become more interesting from the problem solving point of view because the users' background might influence their ideas for new solutions.

The users that answered the quantitative questionnaire on the website are not known and can therefore not be grouped by knowledge or background. Because they are organized in the forum it is likely to say that they have skills in certain areas. As well it is probably more likely that they are willing to take action against VoIP spam. But, they present a group of users that have already experienced spam on the telephone and present the target user group very well.

The authenticity of the research was vividly shown in the harsh reactions of the test users. The information gathered afterwards was reliable due to the users' discussion to the problem. Thus, putting qualitative and quantitative research in relation to each other, the reliability of the research method is underlined. By gathering similar results during the qualitative as well as during the quantitative research it is very probable that a similar research would grant the same results. This also indicates that the methods chosen for the research were reliable.

5.2. Comments

The discussion with the different users who were asked to take part in the research offered a couple of interesting views onto the topic. I would like to present some comments the users added to the research and some comments I received during discussion with test users and others.

First of all the comment by an unknown user was interesting because he held the operator directly responsible for receiving spam:

I have received unwanted calls since I switched the operator; before I was a Telekom (German telephone operator) member and I switched to Arcor (German telephone operator). Until now, the reason for choosing the operator was the expenses; next time I will choose the operator by its annoyance. But how to know this in advance? (Comment from an unknown user)

While all users see the operator as a trustful organisation they probably do not do their job of protecting users. The accuracy of the users comment cannot be vouched for, but it is important to be aware of the fact that this statement could be true.

Another comment was given by a test user who received the test calls that were sent in relation to the thesis. "For a couple of days I have been receiving as many calls as possible; at least 15 a day." Up to this moment the user had actually received seven calls in a time span of 48 hours. Of course, the user might have been exaggerating but the statement still shows that user is annoyed by telephone spam since it features prominently in their daily life

The third comment was copied from the Antispam forum (2007) and is indeed not a unique comment. "Today I was so stupid and answered to the person on the receiving end..." A lot of users fall into the trap of buying something they do not want to buy, mostly because they are taken by surprise. There are a lot of tips how to get out of the trap but it is often a strenuous road the users have to follow. Experienced users recommend not agreeing to anything and never giving away any information.

The last comment is a quite funny story by a user on the Antispam forum.

My friend was called by a trading company nearly every day. They offered commodity future transactions (diamonds, coffee, etc.). Even though my friend was not interested at all he received calls from the same company nearly every day. He set up a meeting and asked a salesman to come by his home at seven o'clock in the morning. The salesman had a couple of hundred kilometres to drive. The salesman went to his house at seven and my friend opened the door and said 'Well, now you can drive home again. Just wanted to see what the person looks like who annoys me every day'. Ever since that day, the company has never called again. (Unknown user on the Antispam forum)

This story is not that unique anymore. More and more users start to take actions against spammers. Often they are not able to harm them but they try to steal some time or annoy the caller by asking silly questions. They describe their actions as well functioning because the caller-companies realize they will not achieve what they want but will spend a lot of time and money by calling those users.

5.3. Further research

Due to the relevance and due to the current situation the research offers a lot of different approaches for further research. Especially users' psychological point of view while answering the telephone or talking on the phone seems to be interesting. The way people interact with their telephone and integrate it into their daily life is important while analysing spam and the rate of annoyance. Moreover, this seems to be an important area for further telephone techniques.

In general, I think that users' habits should be analyzed. They are the key to a solution against spam and they should not be seen as a bulk rather as small parties interacting with each other. Different parties are made up of different individuals who have different habits and needs. By exploring these needs and habits, a more specific technique could be developed that is fine-tuned by every user himself. Due to the need of developing a VoIP spam solution it would be interesting to explore the reverse charge call-solution. Putting this idea in relation to other approaches it could create a new VoIP spam solution while using components of other VoIP spam solutions (pay-per-call, filtering). Due to the level of awareness of the different techniques (because all of them are already well known) users would not be dissociated from the technique.

Another interesting task would be to research not a specific solution but to sort through the ideas and thoughts users post on the internet. Users already provide many different solutions against VoIP spam and they are very creative in creating solutions to the problem of VoIP spam. There surely are some solutions users have developed for their own purposes which already solve the problem of VoIP spam quite well. A research concerning the users' ideas would be interesting for all researchers who develop VoIP spam solutions.

5.4. Summary

In this last part of my thesis I would like to the initial research questions to the results of my thesis. The aim of the research was to analyze and research the users' point of view towards the VoIP spam problem and the extent of users' willingness to disclose private information in order to avoid VoIP spam.

In this thesis the following findings were shown:

- The users' reaction towards VoIP spam was analyzed as well as further actions users took in order to avoid spam.
- Valid research results were gathered. Results from the qualitative research were confirmed by the quantitative research.
- The main points of the results showed that users were not willing to offer private information to companies and that they were not willing to pay any amount of money for VoIP spam solutions. Users held governmental organisations and telephone operators responsible for finding a solution against VoIP spam.

By analysing the results the most promising as well as the most realistic VoIP spam solutions was evaluated. Please see the chapter Appendix for further information about the conducted research.

References

Amazon.com. (2007). Your Amazon.com.

Available on 02. Jun 2007 through:

http://www.amazon.com/gp/yourstore/home/ref=topnav_ys_gw/105-6840219-7183602.

Andersen, Ib (1998). *Den uppenbara verkligheten*. 2nd ed. Lund, Sweden: Studentlitteratur. 85-89.

Antispam. (2007). Forum.

Available on 20. Mar 2007 through: www.antispam.de

Arrison, S. 2004. Canning Spam: An economic solution to unwanted Email [online]. 1st Edition. Pacific Research Institute. 2004.

Available on 20. Jan 2007 through: <http://pacificresearch.org/pub/sab/techno/2004/spam01-26-04.pdf>

Bittner, P. and Hornecker, E. 2005. A micro-ethical view on computing practice. In *Proceedings of the 4th Decennial Conference on Critical Computing: between Sense and Sensibility (Aarhus, Denmark, August 20 - 24, 2005)*. O. W. Bertelsen, N. O. Bouvin, P. G. Krogh, and M. Kyng, Eds. CC '05. ACM Press, New York, NY, 69-78.

Available on 20. Mar 2007 through: <http://doi.acm.org/10.1145/1094562.1094571>

Cerf, V. G. 2005. Spam, spim, and spit. *Commun. ACM* 48, 4 (Apr. 2005), 39-43.

Available on 04. Feb 2007 through: <http://doi.acm.org/10.1145/1053291.1053314>

Electronic Frontier Foundation (EFF). (2007). EFF News and Press Releases.

Available on 20. Mar 2007 through: <http://www.eff.org/>

Gburzynski, P. and Maitan, J. 2004. Fighting the spam wars: A remailer approach with restrictive aliasing. *ACM Trans. Inter. Tech.* 4, 1 (Feb. 2004), 1-30.

Available on 20. Jan 2007 through: <http://doi.acm.org/10.1145/967030.967031>

Good, N. S. and Krekelberg, A. 2003. Usability and privacy: a study of Kazaa P2P file-sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003)*. CHI '03. ACM Press, New York, NY, 137-144.

Available on 20. Jan 2007 through: <http://doi.acm.org/10.1145/642611.642636>

Goodman, J., Cormack, G. V., and Heckerman, D. 2007. Spam and the ongoing battle for the inbox. *Commun. ACM* 50, 2 (Feb. 2007), 24-33.

Available on 20. Mar 2007 through: <http://doi.acm.org/10.1145/1216016.1216017>

Harmonic. (2006). Statistics.

Available on 20. Mar 2007 through: <http://www.citizenonline.org.uk/statistics>

IETF. (2007). Archive of ietf-mxco. Discussion on IETF forum, sponsored by the Internet Mail Consortium.

Available on 01. Jun 2007 through: <http://www.imc.org/ietf-mxcomp/mail-archive/maillist.html#02683>.

ITM GmbH. (2006). Figure H.323 und SIP.

Available on 20. Mar 2007 through: www.itm-group.com/db/voip/IP-6000_a5.gif

ITU-T. (2007). H.323 Packet-based multimedia communications systems.

Available on 16. Jun 2007 through: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-H.323-200107-S!AnnR!PDF-E&type=items

Judge, Paul. 2003. The State of the Spam Problem. *Educause review*. NewHorizons (Sep.-Oct. 2003), 60-61.

Available on 20. Jan 2007 through: <http://www.ciphertrust.com/files/pdf/articles/erm0357.pdf>

Microsoft Corp. (2007). Windows Live Messenger.

Available on 01. Jun 2007 through: <http://get.live.com/messenger/overview>.

Mori, G. and Malik, J. 2003. Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. *IEEE Computer Vision and Pattern Recognition*, 2003.

Available on 20. Mar 2007 through: http://www.cs.sfu.ca/research/groups/VML/pubs/mori-rec_obj-cvpr03.pdf

Ottens, M. (2006). Internetnutzung durch Privatpersonen und Unternehmen. *Statistik kurz gefasst*. 1 (1), 1-7.

Available on 20. Mar 2007 through:

http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-NP-06-012/DE/KS-NP-06-012-DE.PDF

Rosenberg, J. Jennings, C. 2004. The Session Initiation Protocol (SIP) and Spam.

Available on 20. Mar 2007 through: <http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-04.txt>

Satterfield, B. (2006). Ten Spam-Filtering Methods Explained.

Available on 30. Mai 2007 through:

<http://www.techsoup.org/learningcenter/internet/page6028.cfm>

Sherburne, P. and Fitzgerald, C. 2004. You Don't Know Jack About VoIP. *Queue* 2, 6 (Sep. 2004), 30-38.

Available on 20. Mar 2007 through: <http://doi.acm.org/10.1145/1028893.1028895>

Sipgate. (2007). Was ist sipgate?.

Available on 01. Jun 2007 through: <http://www.sipgate.de/user/tour.php>.

Skype. (2007). Skype Home.

Available on 01. Jun 2007 through: <http://www.skype.com/intl/sv/>.

Skype-News. (2005). Who is using Skype?.

Available on 20. Mar 2007 through: <http://www.mathaba.net/news/?x=408348>

TechTarget. (2005). Spitz.

Available on 30. Mai 2007 through:

http://searchvoip.techtarget.com/sDefinition/0,,sid66_gci1024458,00.html

Varshney, U., Snow, A., McGivern, M., and Howard, C. 2002. Voice over IP. *Commun. ACM* 45, 1 (Jan. 2002), 89-96.
Available on 20. Jan 2007 through: <http://doi.acm.org/10.1145/502269.502271>

Appendix

Appendix A: Guideline for the interviews on the qualitative research

New telephone techniques open up the possibility for automated-telephone-calls. Such calls can be very annoying. This research shall clarify if people are willing to offer personal information to avoid unwanted telephone calls.

Unwanted-telephone-calls = commercial calls, telephone marketing, statistical calls etc.
Telephone-call = Fixed telephone call, mobile phone call or computer call (Skype, SIP etc.)

1. Do you receive unwanted-telephone-calls; How many a week?

- None
- 1-5 calls a week
- 5-10 calls a week
- More than 10 calls a week

2. When do you receive unwanted-telephone-calls?

- During Work/School
- During Free time
- During Night

3. How did you react on unwanted telephone calls?

- Listen to the message
- Hung up
- Try to answer
- Did not answer the telephone next time
- Other _____

4. What kind of thoughts did you have after the call (that was fun, hope they won't call again...)?

5. Was your daily life disturbed by such calls? In what way?

6. Did you have any costs by receiving unwanted-telephone-calls?

- Voice mail (Costs for calling the voice mail)
- Cost for roaming (Receiving calls outside the country)
- Forwarding costs
- Other _____

7. Have you tried to get rid of unwanted-telephone-calls? What did you try to do?

8. Within a week, how many unwanted-telephone-calls would you accept?

- None
- 1-5
- 5-10
- I do not care

9. Would you pay a monthly amount to get rid of unwanted-telephone-calls? How much? (Take into account to receive spam on the voice mail or in another country)

- Less than 10 SEK a month
- 10-50 SEK a month
- More than 50 SEK, as long as I get rid of it

10. Would you give up anonymity to avoid unwanted-telephone-calls? To whom? Who may save your personal information to avoid unwanted-telephone-calls? Fill in following table:

	Government	Service Operator (Telia, T-Mobile, Skype, Sipgate)	Companies / Systems (OpenID, Microsoft, Google)	Organisations (W3C, ICANN, NIX)	No one
Name					
Social security number					
Residence information					
Telephone records					
Credit Card Information					
Bank account numbers					
internet history					
IP address					
date, time and duration of your calls					

If you would receive the same amount of unwanted-telephone-calls on a long term (a year) as you received during the last week.

11. Do you think that unwanted-telephone-calls would influence your daily life? How? Would you use your telephone differently than you do today?

12. From your point of view: who should develop unwanted-telephone-calls solutions and why?

13. Do you use Skype or any SIP telephone?

- Yes, often
- Sometimes
- No, never

14. Do you buy on the internet (Amazon, CDon, ebay)?

- Yes, often
- Sometimes
- No, never

15. Sex

- Male
- Female

16. How old are you?

- 15-20
- 20-30
- 30-40
- 40+

Appendix B: Questionnaire for the quantitative research

Due to the fact that this research took place on the German website Antispam (2007) the questionnaire was published in German.

Unerwünschte Anrufe = Telefonmarketing, Vertrieb via Telefon, Untersuchungen etc
Anruf = Anruf auf Festnetztelefon, Mobiltelefon, Sip-Telefon

1. Wie viele unerwünschte Anrufe erhalten Sie im Monat?

- Keine
- 1-5 Anrufe im Monat
- 5-10 Anrufe im Monat
- Mehr als 10 Anrufe / Monat

2. Wie reagieren Sie?

- Lege einfach auf
- Suche das Gespräch mit dem Anrufer
- Hebe beim nächsten Anruf nicht mehr ab
- Anderes:

3. Wird ihr tägliches Leben (beruflich als auch privat) durch Telefonanrufe gestört?

- Nein, eigentlich nicht
- Nur wenig
- Ja gelegentlich
- Ja sehr, beeinträchtigt mein Leben permanent

4. Haben Sie aktive Maßnahmen ergriffen / versucht zu ergreifen um gegen die Anrufe vorzugehen?

- Nein, nichts unternommen
- Habe die Polizei hinzugezogen
- Habe meinen Vertragspartner angerufen
- Habe das Telefon gelegentlich ausgeschaltet
- Nehme nur noch Anrufe angenommen bei welchen die Nummer angezeigt wurde
- Anderes

5. Wer sollte Ihrer Ansicht nach Lösungen entwickeln um gegen ungewollte Telefonanrufe vorzugehen?

- Telefongesellschaften
- Staatliche Organisationen
- Private Unternehmen
- Egal, Hauptsache es findet sich eine Lösung
- Keiner der angegebenen Organisationen / Unternehmen

6. Würden Sie Teile Ihrer Privatsphäre an dritte weiter geben, um damit sicher zu stellen keine ungewollten Anrufe mehr zu erhalten?

	Staatliche Organisationen	Telefongesellschaften	Privaten Unternehmen	Niemandem
Name				
Wohnadresse				
Residence information				
Telefon-Historie				
Kreditkartennummer				
Kontonummer				
IP-Adresse				

7. Würden Sie einen monatlichen Beitrag zahlen um keine ungewollte Anrufe mehr zu erhalten? Wie viel? (Vergessen Sie nicht die Kosten welche beim Empfang durch ungewollte Anrufe entstehen; Roaming, Mailbox, Arbeitszeit etc)

- Weniger als 1 Euro im Monat
- 1- 5 Euro Euro im Monat

- 5-20 Euro im Monat
 - 20 - 100 Euro im Monat
 - Mehr als 100 Euro im Monat, Hauptsache keine ungewollten Anrufe mehr
8. Benutzen Sie Skype oder Sip-Telefon?
- Nein, nie
 - Manchmal
 - Ja, oft
9. Kaufen sie Produkte im Internet?
- Nein, nie
 - Manchmal
 - Ja, oft

Appendix C: Texts Voice Commercials

Want to stop waking up during the night by telephone? Buy the new spam filter from antispam! Costs only 15 dollar per month and detects more than 99% of all calls! Call now 01902229933 or stay on the line to get connected with a dispatcher!

Hatar du oväntade samtal? Vill du stoppa dem? Besök var hemsida på www.spamiswhatihate.com och registrera ditt nummer för att stoppa sadana samtal! Och vi lovar att aldrig ringa igen....

Sound

You wanna to pleasure your girlfriend a bit more? You have some tiny problems with your HARDware? We got a solution for your problem.

Order our package, that includes:
 30 pills for one month
 A Swedish pump
 Educational german movies
 Some training magazines
 And our book "get larger in one month"!

Call today 071-66 66 66 or order directly at www.billybooper.com with credit card, växjö student id or your last bus ticket.

Hej,

Söker du jobb? Är du kommunikativ, kan prata i telefon och ser bra ut? Vill du tjäna mer än 10.000 kronor i månaden?

Jobba hos www.gordetsjalv.se och sälj vara produkter till människor från hela sverige.

Vi ska informera dig varje vecka om nya anställningar. Vill du inte ha mer information? Ring 076 80 13 36 och säg upp dig från listan.

Hallo, mein Name ist Günther G,!

Herzlichen Glückwunsch - Du hast einen neuen Ferrari Meranello gewonnen! Dieses wunderbare Auto kannst du dir nun abholen. Du brauchst nur auf unsere Website www.millionengewinner.de gehen und deinen gewinnercode eingeben. Der code lautet wie folgt: XPR32P . Wiederholung: XPR32P.

Wenn du noch andere tolle preise gewinnen willst registrier dich auf millionengewinner.de
und staub ab was das zeug hält!

Want to be a member of a golf club, get an American gold card and wear Gucci all day long?
Call now 071 99 22 33 and become a member of one of the top 10 platin clubs in Europe!
FOR FREE! Only today and only right now. 071 99 22 33 – now or never. Plating club
Europe!



Växjö
University

Matematiska och systemtekniska institutionen
SE-351 95 Växjö

Tel. +46 (0)470 70 80 00, fax +46 (0)470 840 04
<http://www.vxu.se/msi/>