Analysis of spam over Internet telephony protection techniques

Vincent M. Quinten
v.m.quinten@student.utwente.nl

ABSTRACT

Spam in Internet telephony networks is likely to become a large problem in the future, as more and more people and companies switch from traditional telephone networks to Voice over IP (VoIP) networks. VoIP spam is likely to have a great strain on the network.

The question that will be answered in with this research is: “What methods exist against spam over Internet Telephony and which technique or combination of techniques is the most promising for the future?” Therefore, we identify techniques to prevent and reduce spam in VoIP networks that exist today. These techniques are analyzed for their advantages and disadvantages and on how they comply with criteria that spam protection techniques have to meet. We also identify some combinations of techniques that would complement each other. This will provide an overview that can be used for other research on the topic of VoIP spam.

We identified a technique that is suitable for use, memory bound functions. In addition, a combination of this technique with whitelisting or signaling protocol analysis with whitelisting are promising for the future? Therefore, we identify techniques to prevent and reduce spam in VoIP networks that exist today. These techniques are analyzed for their advantages and disadvantages and on how they comply with criteria that spam protection techniques have to meet. We also identify some combinations of techniques that would complement each other. This will provide an overview that can be used for other research on the topic of VoIP spam.

We identified a technique that is suitable for use, memory bound functions. In addition, a combination of this technique with whitelisting or signaling protocol analysis with whitelisting are suitable for use as protection techniques against VoIP spam.

Keywords
Voice over IP, spam, sp, Internet Telephony, Spam over Internet Telephony

1. INTRODUCTION

Voice spam is defined as unsolicited bulk calls each resulting in a media session, where the content delivered to phone or voice terminal may include voice, images or video [MV05]. There are several different kinds of voice spam, i.e. advertisement, telephone polls and telemarketing. Voice spam is also known as spam over Internet telephony (SPIT).

The next section describes the problem statement, followed by the goal of this paper in section 1.2. Section 1.3 describes the approach used for the research and section 1.4 describes the outline of this paper.

1.1 Problem statement

The usage of Voice over Internet Protocol (VoIP) is growing fast, it is estimated that in the year 2010 25% of all households in Western Europe have abandoned traditional public switched telephone network (PSTN) services in favour of VoIP [Ele05]. With the growth of VoIP communication, the misuse of VoIP will grow also. There is a fear that advertisers will send numerous voicemail messages to VoIP users, therefore causing a reduction in bandwidth and breaks in the service. VoIP spam will have a much greater strain on the network in comparison to e-mail spam, because the average message size of VoIP communication is about ten times larger compared to an average e-mail message [Gag05].

Compared to e-mail spam, VoIP spam is more obtrusive [PS05]. With e-mail, the user decides when he is going to read his messages, but with VoIP, the phone will ring with every spam message, even in the middle of the night when you are asleep. So VoIP spam will interfere with the user’s current activity every time the phone rings.

The use of VoIP instead of traditional PSTN networks will also make it easier for spammers to make automated tools to deliver their spam to the user [MV05]. VoIP is also a lot cheaper compared to traditional PSTN telephone, both the monthly fee as well as the costs per call are cheaper. The authors of [RJ04] claim that the costs per call for VoIP are roughly three orders of magnitude cheaper than traditional PSTN calls, making it a lot cheaper for a spammer to get his message out into the world.

The two main protocols used in VoIP are the H.323 protocol and the Session Initiation Protocol (SIP), both protocols are equally vulnerable for spam, because of implementation errors and protocol features that are exploited [Edo05]. Because the main VoIP protocols are equally vulnerable to spam, they have been left out of the analysis described in this paper.

1.2 Goal

The goal of this paper is to present a state of the art overview of techniques used to prevent or mitigate spam in VoIP networks, including an analysis of the technique or combination of techniques that are most promising for the future. This overview can be used as a reference by other researchers, who want to develop new VoIP spam prevention techniques or improve existing techniques. Such an overview was not available at the time of writing. However, two papers exist which present some related work. In [RJ04] some techniques are discussed with their advantages and disadvantages, this paper however only contains a small selection of spam protection techniques and aims at SIP techniques. A selection of the techniques described in this paper is also described in [Rad05], but does not provide criteria where the analysis is based on.

The question that will be answered in this paper is: “What methods exist against spam over Internet Telephony and which technique or combination of techniques is the most promising for the future?”

1.3 Approach

To answer the research question, a study of the existing literature on the topic of VoIP spam has been conducted. The criteria that spam prevention techniques have to meet have been extracted first from this literature. These criteria are needed to compare the different techniques with each other. After the extraction of the criteria from the literature, the advantages and disadvantages of each technique have been extracted.
Next, an analysis of the techniques listed is performed. This analysis is based on the criteria identified, the advantages and disadvantages of each technique and partly based on existing analysis from the literature. The last step was to define which techniques or parts of techniques must be improved in the future, to make the techniques more effective in preventing spam in VoIP networks.

1.4 Outline
The criteria used to compare the different technologies with each other are described in chapter 2. Chapter 3 lists the prevention techniques with their advantages and disadvantages. The analysis of the techniques is described in chapter 4. Chapter 5 describes further work that needs to be done to improve the prevention techniques and to make spam prevention more effective. Finally, chapter 6 contains the conclusions of the research.

2. CRITERIA
For a VoIP spam mitigation technique to be effective and user friendly, it needs to meet a number of criteria. This section will discuss the most important criteria that have been distilled from literature on the topic of VoIP spam.

A very important criterion is that the technique has to identify spam before the phone at the end-user rings [MV05]. This is important, because if the telephone rings this will disturb the current activity of the end-user. In case of spam, this will cause a loss of productivity. It is extremely disturbing for the end-user when the telephone will ring because of spam, for example in the middle of the night when the call wakes up the end-user.

Another important criterion is the need for user intervention for the maintenance of the VoIP spam protection technique. The less maintenance needed to be done by the user the better, because this means that it will not interfere with the normal activities of the user [PS05].

The cost involved with the spam protection technique for the users is also an important aspect. It is preferable that a spam protection technique involves as less costs as possible for the user. From the users perspective it is also preferable for a protection technique to raise the costs for the spammer as much as possible, because this means that spamming will be less profitable for the spammer. When spamming becomes less profitable it will eventually lead to less spam [Har03].

The number of false positives and false negatives should be as small as possible, preferably even zero, for a spam protection technique. This is important because for many businesses and also home users telephone calls are very important. For businesses it’s even essential that potential customers can reach the company [MV05].

The delay of the call caused by the spam protection technique is also an important factor to consider [PS05] [Har03]. The less delay caused by the technique the better, preferably the technique does not cause any delay at all.

And last but not least the ability to circumvent the blocking by a spam technique is very important. If a technique is very effective in detecting spam, but is easy to circumvent, the technique will soon be circumvented by all spammers and will have no effect at all [Har03]. An effective spam protection technique should be both effective and very difficult to circumvent.

3. TECHNIQUES
Based on the criteria defined in the previous section we will now discuss a number of techniques. For each technique the advantages and disadvantages are discussed.

3.1 Signalling Protocol Analysis
VoIP calls consist of two parts: signalling and media data. Before every VoIP call signalling data for setting up a call is exchanged between the two end-users. Spammers are interested in the correct delivery of their calls, therefore the call routing information provided in the call setup request is valid and can therefore be used for further analysis. A second characteristic of spam calls is that they are unidirectional: the spammer initiates the calls to the targeted network, but nobody calls the spammer. A third characteristic is the termination behaviour, this is statistical consistent. This means that there is a pattern of which of the two calling parties terminates the call. A fourth distinction is, spammers do not call the same recipient for some period of time. Based on these characteristics of voice spam calls, the authors of [MV05] define a number of scenarios for the statistical termination behaviour that can be distinguished.

Based on a statistical analysis of this termination behaviour the authors claim that it is possible to achieve an accuracy of about 99.9%.

A great benefit of this technique is that it decides if the call is a spam call before the phone at the receiving side actually rings. This means that spam calls will not interrupt other activities of the receiver when this technique is used. A second benefit is that the system is located at the service provider, so it does not require maintenance of the end-user.

The big disadvantage of signalling protocol analysis is that it is only reliable enough after about ten calls from a certain user. So the first ten calls of a spammer will succeed and only after these calls the signalling protocol analysis will be able to detect spam. The authors make the assumption that the spammer does not change his number for a longer period of time, but in reality it is very simple to request a new phone number in VoIP systems, as long as this is the case a spammer will be able to easily circumvent the system by changing his phone number after for example every ten calls. Another disadvantage of signalling protocol analysis is that legitimate services will also be blocked, for example an automated system of a bookstore that will inform you that your book has arrived will also be blocked by signalling protocol analysis.

This technique is relatively new, there is only one article [MV05] published about signalling protocol analysis to prevent spam in VoIP networks. The available article about this technique is only theoretical and does not contain any practical test results.

3.2 Do not call register
A do not call register is an initiative of the Federal Trade Commission in the United States of America. Users can register their phone number in the register. Most telemarketers have an agreement with the do not call register that they will not call the users that are registered in the do not call register.

A do not call register can be controlled nation wide, so the user only has to register his phone number once and the organization that controls the do not call register will handle the rest of the administration, this will mean minimal user intervention [FTC05]. For the telemarketers that have agreed not to call the registered users there is a quite large penalty if they do actually
call a registered user. This penalty enforces the effectiveness of the register [Edw02].

The main disadvantage of a do not call register is that there has to be an agreement with the telemarketers, so do not call registers may not be obeyed by spam sources outsourced offshore [MV05]. This means that when some telemarketer calls from another country that doesn’t have such a register, they are able to keep spamming without any consequence. With the use of VoIP this scenario is not very unlikely because the costs for calling to another country are much less than the costs for a normal PSTN call.

Another disadvantage are the costs involved with checking if telemarketers obey the do not call register. An investigation is needed when a certain amount of complaints have reached the control organization. These costs are eventually paid by the taxpayer and not by the one that makes the unwanted calls, the spammer [Edw02].

Circles of trust, as described in [RJ04], is another technique that is very similar to a do not call register. Companies agree to exchange VoIP calls amongst each other and also agree to introduce a fine should one of them being caught spamming. Each company enacts measures to terminate employees who spam from their account. Circles of trust work well on small domains, but it is unknown how they would scale in large domains.

### 3.3 Whitelisting

Whitelisting is a technique primarily used in instant messaging networks. In case of VoIP a whitelist contains the telephone numbers of the people that are allowed to call you. When anyone whose telephone number is not on the whitelist tries to call you he is blocked. The great benefit of a whitelist is that it will in theory block all spam calls, when we assume that nobody on your whitelist is a spam source or will become one [Rad05]. But this benefit has also a great disadvantage, when someone new to you wants to call you, but his phone number is not on the whitelist his call will be blocked. Some home users don’t think about this as being a disadvantage. But in case of business users this is a great disadvantage, because new customers will not be able to contact the company [Rad05].

On the other hand the user has complete control about who can call him and who can’t, this will be a benefit for some home users [Rad05]. But this control comes with a price, because the user will be responsible for the maintenance of the whitelist, which will be a considerable amount of work if you have to enable new people to call you, but this will not be a big issue for users that have an almost constant whitelist, with limited changes once in a while.

Whitelists are not as easy to circumvent as other VoIP spam protection techniques, because a change of identity of the spammer will not work to circumvent a whitelist [RJ04].

### 3.4 Blacklisting

The complete opposite of whitelisting, as discussed in the previous section, is blacklisting. Instead of maintaining a list of the phone numbers of the people that are allowed to call you, you maintain a list of the phone numbers of people that are not allowed to call you.

For a blacklist to be effective you need to implement it on a global level. When separate users all have their own blacklists which differ from user to user they have very limited effect. Only when you implement blacklists on a global level the costs can raise that much for the spammers to make spamming unprofitable [Rad05]. This global blacklist should be maintained by a non-profit organization to prevent a commercial organization to make huge profits on this. Everybody must be able to add a number to the blacklist to make it effective. On a global scale this should be done by adding a phone number after a certain number complains about the same phone number [Rad05].

Another great disadvantage is the fact that the user first has the answer the call before he can decide if this number should be blocked or not, so spam will continue to arrive at the user until the number has been added to the blacklist. This can mean a considerable amount of work for the user if he receives calls from many different sources. And even when a number has been added to the blacklist this can have some unwanted side effects. When a spammer makes use of a proxy for his VoIP communication all users behind this proxy will be blocked instead of only the spammer. Which will result in the fact that many other users will also be unable to contact you [RJ04] [Rad05].

Blacklists are very easy to circumvent with VoIP, because it’s very easy and inexpensive to request a new VoIP number when your number has been added to a blacklist. As long as it’s very easy and inexpensive to request a new VoIP number blacklists will not have much effect, because spammers will request a new number as soon as they are added to a blacklist [Rad05] [Har03].

### 3.5 Greylisting

Greylisting is based on a simple rule that is applied to all incoming messages: each incoming message will be blocked unless the same IP address has tried to establish a call within the last N hours/minutes. When the sender is blocked, he will receive a message like “the user is currently busy”. Normal users will then try to call back later. After the sender has called back his IP address is added to the whitelist and all future calls will be connected immediately.

A great benefit of this system is the automatic maintenance, this causes very little work for both the administrator of the system and the user [Har03]. When the used VoIP protocols are implemented correctly this techniques does not have any false positives, which is a great advantage, because this means that no calls will be blocked that should have reached the user [Rad05] [Har03]. The use of Greylisting makes that the spammer needs more bandwidth and makes more costs, because if he wants to make a successful spam call he needs to call every user at least twice within the N hours/minutes time period. This makes spamming less profitable for the spammer and will eventually result in a drop in the number of spam calls in VoIP systems [Rad05]. Trying to circumvent Greylisting has no effect or even an opposed effect, because this will make Greylisting or other techniques even more effective. For example when a spammer requests a new IP address to circumvent the greylist this means that this new IP address is not on the users whitelist which means that the spammers should again call at least twice to make a successful call to the user, adding additional costs for the spammer [Har03].

A disadvantage of the system is that it is designed as a system complementary to existing systems and not to replace any systems, this means that you also need other protection techniques [Har03]. For some users, especially some business users, the fact that the setup of a call will take longer, because the first attempt will be rejected will be a great disadvantage. But for most private users this will not be a great sacrifice if they know that spam will be eliminated [Har03]. The technique
is also not suitable for emergency calls or other urgent calls, because of the delay caused by the first rejection of the call [Rad05]. A technique similar to Greylisting is described in [CO05].

Consent based communication [RJ04] is a technique very much like Greylisting, the only significant difference is that the user has to accept the caller manually on the second call instead of automatically. This causes an extra way to circumvent the technique by spamming the user with consent requests instead of the spam calls [RJ04]. Because of the many similarities of consent based communication and Greylisting, consent based communication is not listed as a separate technology.

3.6 Rate limiting
Rate limiting allows the user to make a certain amount of calls per day. When the user makes more calls as the limit that is set, the user is likely to be a spammer and the user will be blocked. This is a very simple technique that does not bother the average user, when the limit is set at the correct level, but will limit spammers in their ability to send spam [Rad05].

The main disadvantage is that this technique has to be supported by all service providers world wide, because if it’s not spammers will easily change to a service provider that’s more spam-friendly, in the fact that they do not have a limit. In this case rate limiting is very easy to circumvent and will have no effect [Rad05].

3.7 Reputation filtering
Reputation filtering is based on scores that have been given to a user by other users. Reputation filtering allows users to either praise each other or to give each other negative reputation scores. This reputation can be used by other users to decide to allow the calling user or to deny his calls. When the receiving user decides to allow calls, he adds the phone number to his whitelist. For example, when user A tries to contact user B and user A is not on the whitelist of user B, a client can request the reputation score of user A to user B. This reputation score can help user B to decide if he wants to add user A to his whitelist or not. When user A has a bad reputation user B can decide not to allow calls from user A.

A great disadvantage of reputation filtering is the ability for spammers to cheat, when spammers have many telephone numbers they can help each other to receive a good reputation. This will actually circumvent the system, making it useless [RJ04].

Reputation filtering works fine for small networks, but for large networks the search paths for reputations become very long, causing long delays, which is not preferable for the user [RS05]. The user also needs a buddy list which he must maintain and give a reputation for every person that will call him. This can become very intensive for the user [RS05].

3.8 Handshake/Challenge/Turing test
Handshake/challenge/Turing tests are depending on the fact that some things are easy to do for humans, but almost impossible to do for a computer. This system is for example used in e-mail systems, where the user has to recognize some letters from a picture with a lot of background noise [RJ04]. A human user can easily distinguish the letters from the background noise, but a computer using optical character recognition will fail on this. However, there are systems that are able to circumvent handshake/challenge/Turing tests in e-mail systems, as described in [Hoc05].

Handshake/challenge/Turing tests can also be adapted for the use in VoIP networks [RJ04], where a user for example has to solve a little math question that is spoken out when he tries to call someone and pass back the correct answer. When the user provides the correct answer, he is instantly connected to the receiving user. Since voice recognition is extremely difficult for computers using techniques available nowadays, this system will hold off automated calls. With today’s technology, a huge amount of computer power will be needed to circumvent this for every call, making spam unprofitable for the spammer.

When speech recognition becomes more advanced, the system will be easy to adapt, by making the questions more difficult for a computer. For example you could ask questions like: “What’s the capital of Italy?” this will be very difficult for a computer to answer.

In contrast with Greylisting and memory bound functions with handshake/challenge/Turing tests the call will not lose it’s instant character, because the test will cause almost no delay for a human user [Rad05].

A disadvantage of the use of a system that’s based on speech is that it will not work very well for companies that take calls from different countries with different languages. The system could make use of an English voice, but this could not be understand by all callers [Rad05].

This system relies for a big part on the acceptance of users. It can lead to irritations of the callers, which could lead to the early termination of the call, even before the called party answered the call. This will not be very attractive for most businesses [Rad05].

3.9 Payment-at-risk
Payment-at-risk tries to make spam more expensive for the spammer, but minimize the costs for the user. To achieve this, the calling party has to make a small deposit to the called party before the calling party can make the call. This deposit can be e.g. 5 cents, and it will be refunded by the called party if the call is not qualified as spam [RJ04]. So a spammer will not be refunded by the called party, increasing the costs for the spammer, because the spammer needs to pay for the call and also pay the extra 5 cents for every call he makes. These extra costs will make spamming less profitable for the spammer, and should cost a normal user theoretically nothing. The problem with this system though is the costs that are charged for the micro payments, these costs are relatively large compared to the amount transferred. The costs of micro payments makes that normal users also lose money with every transfer, adding additional costs for him. As described in [RJ04], the traditional costs for internet payments are around 25 cents per transaction, this is five times as expensive compared to the deposit of 5 cents. Recently providers have been willing to charge 15% of the transaction for small transactions. These costs have to be paid by the users of the system.

The following example from [RJ04] makes an estimation of the costs for a normal user. Let’s assume a busy user that receives about 10 calls a day from unknown senders that are not on the user’s whitelist. If the deposit made is 5 cents, the transaction provider would take 0.75 cents and deliver 4.25 cents. If the sender is allowed, the recipient returns 4.25 cents, the provider takes 0.65 cents and returns 3.6 cents. This costs the sender 0.65 cents on each transaction if it was a legitimate call. If there are ten new recipients per day, this will cost about 1.95 a month, which is relatively inexpensive.
3.10 Content filtering
Content filtering for VoIP calls is done by the use of speech recognition technology to analyze the content of the message and decides based on the extracted content if the message is spam. The main disadvantage of this system is that it is impossible with today’s technology to analyze the content of a VoIP call in real-time [RJ04]. Also some VoIP providers use some kind of encryption for extra security [Sky06].

When a system based on content would work, it is very simple to circumvent by spammers, simply by the use of an accent or by using bad grammar [RJ04].

Another major disadvantage of content filtering is that it does not work before the user answered the call. The user is already paying attention to the call before content filtering can do anything [RJ04].

3.11 Memory bound functions
The basic idea of Memory bound functions is: “If I don’t know you and you want to send me a message, then you must prove that you spent, say, ten seconds of CPU time, just for me and just for this message” [DGN03]. This “proof of effort” is mainly cryptographic, it’s hard to compute but very easy to check.

Memory bound functions are implemented at the service provider and need the user to do some complex computation before the user is allowed to make the actual call. This complex computation will consume computing power at the senders’ device for every call he wants to make. For spammers this means that they need much more hardware to make the same amount of calls, because of the computer power consuming computation. This will make it very expensive for a spammer to make a huge amount of spam calls in a short time, while the average user will not be bothered [Rad05]. A spammer also has to pay for the extra calling costs that are made while the computation is solved.

The extra costs involved with memory bound functions could make spam unprofitable and this could be a definitive solution to the spam problem according to [Rad05].

Another advantage of memory bound functions is that normal calls are not blocked and it is still possible to make legal advertisement calls, because a delay of say ten seconds is not a big restriction for a normal callcenter [Rad05].

The main disadvantage of the use of memory bound functions is that all calls are delayed for some time, depending on the calculation time defined by the service provider. This makes the system completely unacceptable for urgent calls and emergency calls [Rad05].

4. TECHNIQUE ANALYSIS
This chapter contains the results of the analysis of the techniques described in chapter 3, this analysis is based on the criteria defined in chapter 2.

Section 4.1 contains the results of the analysis of the VoIP spam protection techniques described in chapter 3 as a single stand-alone technique. Section 4.2 describes the results of the analysis of combinations of certain techniques from chapter 3 that cancel out each others disadvantages.

Because at the time of writing for most described techniques no figures about the amount of false positives and false negatives of these techniques in VoIP networks were available, the criterion of false positives and false negatives is meanly left out of the analysis.

4.1 Single technique
This section contains an analysis of the VoIP spam protection techniques as stand-alone technique based on the criteria defined in chapter 2. There are three categories of techniques identified, first section 4.1.1 describes the techniques that are unsuitable for protection against VoIP spam. Section 4.1.2 describes the techniques that show potential to become a good technique against VoIP spam or a technique that will work well in combination with other techniques. Section 4.1.3 describes techniques that are suitable as a stand-alone technique to prevent VoIP spam.

4.1.1 Unsuitable techniques
This section describes techniques that have been identified as unsuitable to protect against VoIP spam, according to the criteria defined in chapter 2. For each technique is described why the technique is unsuitable.

4.1.1.1 Content filtering
Content filtering is classified as an unsuitable VoIP spam protection technique, because it works only after the user has picked up the phone. This means that VoIP spam will still disturb the user’s current activity.

The technology needed to perform content filtering on voice is not available today and it would require enormous amounts of computer power to perform this. Even when the technology needed for content filtering was available it would be very easy to circumvent as described in section 3.10. When service providers use encryption for VoIP, this would add extra difficulties to perform content filtering, if not making it impossible.

4.1.1.2 Do not call registers
Do not call registers are not suitable as a solution against VoIP spam. Do not call registers are based on agreements between companies, participating companies agree that they do not call the registered users. Spammers will very likely not join these kinds of agreements, because the goal of spammers is to get their message out to as many persons as possible. It is also possible that the spammer will outsource his calls to other countries that do not have do not call registers. With VoIP making international calls cost only a fraction of the costs of international calls via the traditional PSTN. These lower costs make it more likely that this scenario will take place. So the technique is relatively easy to circumvent by the spammer.

Checking if participating companies fulfil the requirements of the agreement they made for the do not call registers also involves high costs. These costs eventually have to be paid by legitimate users, instead of by the one that sends the spam messages. So this technique does not meet the criterion that the costs for the user have to be as low as possible and the costs for the spammer as high as possible.

4.1.1.3 Reputation filtering
Although reputation filtering works fine for smaller networks, it does not scale well for larger networks. In large networks the search paths become very long, causing long delays, which is according to the criteria defined in chapter 2, unwanted. Reputation filtering also doesn’t fulfil the criterion of minimal user intervention, because for every, until then unknown, caller the user has to decide if he wants to allow the call based on the reputation of the caller. When the caller is accepted he has to be added to the user’s whitelist. This can be a lot of work, for users that receive a lot of calls from unknown callers, for example businesses.
Reputation filtering is also sensitive for circumvention, because in large spam networks, spammers can help each other to get a high reputation by giving each other a positive mark.

4.1.1.4 Rate limiting
Rate limiting is an unsuitable technique for VoIP spam protection, because it does not fight spam, but only limits the spammer in the amounts of messages that he can send. This is also easy for a spammer to circumvent, by just switching to a more ‘spam friendly’ service provider.

4.1.1.5 Blacklisting
Blacklisting does not meet the criterion that the technique needs to work before the phone rings, because before the user can add somebody to his blacklist he first needs to answer the call to decide if it is spam. When the user receives a considerable amount of spam calls from different sources the adding to the blacklist can be a considerable amount of work for the user, which is unwanted according to the criteria from chapter 2.

For a blacklisting system to work the system needs to be implemented on a global scale, which requires a complex maintenance system. This would probably involve high costs that need eventually to be paid by the user, which is in conflict with the criterion that the spammer should be the one with the high costs.

The system has an unwanted side effect, when a proxy server is added to the blacklist all other users who are behind that proxy are blocked, not only the spammer.

Blacklists are also very easy to circumvent, when the spammer requests a new phone number, he is not on the blacklist and can continue until he is added again to the blacklist.

4.1.2 Techniques with potential
This section describes the techniques that show potential to become a suitable technique against VoIP spam or a technique that will work well in combination with other techniques.

4.1.2.1 Whitelisting
Whitelisting is not a very practical technique for users that receive calls from several new callers, because before the new caller is able to call, the user first has to add him to the whitelist. Especially for businesses this is not desirable, because new customers are not able to call them. Also there would be a large amount of maintenance needed to maintain the whitelist.

But whitelisting meets some of the criteria of chapter 2, namely it works before the phone rings, is difficult to circumvent and causes no delays.

Especially in combination with other spam protection techniques whitelisting can be very effective, as described in section 4.2.

4.1.2.2 Signalling protocol analysis
Signalling protocol analysis is a new technique, there is only one paper published about it. This paper contains only theoretical data, but when this theoretical data also holds in practice signalling protocol analysis has the potential to become a good spam protection technique. This technique works before the phone rings. The technique is located at the service provider, so the user has no maintenance. It causes no delay and has a high effectiveness of about 99.9% according to the authors of [MV05]. The number of false positives could be lowered if the technique is used in combination with whitelisting as described in section 4.2.

This technique would benefit greatly, if it would be harder to request a new telephone number, because the technique works after the first ten calls made by the spammer. When it is more difficult to request a new telephone number it will be more difficult to circumvent this technique.

4.1.2.3 Payments at risk
Payment at risk places the bill at the place where it really hurts, at the spammer. This would raise the costs of spamming for the spammer a lot, but the costs for the normal users is almost nothing. The aim of this technique is to make it for the spammer unprofitable to send spam and prevent spam in the future. This will attack the spam problem at the source.

Payment at risk needs some of the user’s attention, because at the end of the call the user has to decide if he wants to refund the deposit made by the caller.

Although this technique does not meet all criteria, it is identified as a technique with potential, because it attacks the spam problem at the source and makes it less attractive to spam.

4.1.2.4 Greylisting
Greylisting is a technique that is designed to complement existing spam protection techniques, but it has a lot of potential. Greylisting works before the phone rings, because it automatically denies the first call of a caller. Greylisting also increases the costs for the spammer, because everyone that he tries to call needs to be called at least twice. When the spammer tries to circumvent greylisting, other techniques that are used together with greylisting become even more effective [Har03].

A disadvantage is the delay caused by greylisting because the first call attempt is rejected. This disadvantage can be prevented by combining greylisting with other techniques, as described in section 4.2.

4.1.2.5 Handshake/Challenge/Turing test
Handshake/Challenge/Turing tests, further referred to as Turing tests, are relatively similar to memory bound functions in some ways. Both techniques ask the calling party to answer some question, but the way this is done differs. Memory bound functions require the calling party to do some complex cryptographic calculation, that take a predefined time. Turing tests ask the calling party a simple voice system based question.

Turing tests fulfil also most of the criteria defined in chapter 2. Turing tests do their work before the phone at the receiving side rings. Turing tests need a huge amount of computer power to circumvent, adding costs for the spammer. Even when a spammer is able to circumvent the Turing test, in the way that he can provide the correct answer to the asked question, Turing tests are easy to upgrade to questions that are more difficult, as described in section 3.8. However, Turing tests expect a certain level of knowledge of the user. For example, when a child tries to call her father at work, she has to answer a question and provide the right answer. If the question is too difficult, she is not able answer it and thus not able to call her father. But if the question is to simple, spammers will also be able to answer the question with a voice recognition system, making the technique ineffective. Another problem that arises when questions become more difficult, like “What is the capital of Italy?”, is that the buttons of the telephone can become insufficient to supply the answer. In that case a voice recognition system is needed to verify the answer, which causes the same difficulties for the party that verifies the answer as it would for a spammer to do voice recognition.

The use of Turing tests cause a small delay for a human user, this can lead to irritations of the callers. This delay can be solved by combining Turing tests with other spam prevention techniques. This technique would benefit greatly, if it would be harder to request a new telephone number, because the technique works after the first ten calls made by the spammer. When it is more difficult to request a new telephone number it will be more difficult to circumvent this technique.
techniques as described in the next section. The language used for the Turing tests can become a bit of a problem for large international companies, because not all customers will speak the same language, the solution for this requires further work.

4.1.3 Suitable techniques
This section describes the techniques that are suitable to use against VoIP spam. For each technique an argumentation is given why the technique is identified as a suitable technique.

4.1.3.1 Memory bound functions
Memory bound functions fulfill almost all criteria that are defined in chapter 2. Memory bound functions work before the phone rings, so the user is not disturbed in his current activity. As described in section 3.11 memory bound functions increase the costs for the spammer, making spam less profitable. Memory bound function systems are located at the service provider, so no user maintenance is required.

The criterion that is not met by memory bound functions is that memory bound functions cause delays in all calls, but as described in section 4.2 this can be solved relatively easy.

4.2 Combination of techniques
This section contains an analysis of the VoIP spam protection techniques as a combination of different protection techniques. These combinations of spam protection techniques cancel out most of each others disadvantages.

4.2.1.1 Handshake/Challenge/Turing Tests in combination with Whitelisting
The combination of handshake/challenge/Turing tests with an automatically maintained whitelisting will cancel out most of the disadvantage of user acceptance. When a caller passes the handshake he could be automatically added to the user’s whitelist, this will result in a system where the caller only has to meet the handshake once, instead of every time he calls. This also solves the knowledge problem as described in section 4.1.2.5 partially, because the question has to be answered only once.

A possible disadvantage of this is that spammers could adapt this system and invest the time and costs to meet the handshake once and afterwards being able to spam the user as much as he wants [Rad05]. This scenario can be countered by adding an expiration time to the records on the whitelist, because one of the characteristics of VoIP spam is that the same user will not be called by a spammer for an extended period of time, as described in section 3.1. The expiration will remove the spammer from the user’s whitelist, so he has to meet the handshake again the next time he calls the user.

4.2.1.2 Memory bound functions in combination with Whitelisting
The delay caused by memory bound functions can be partly cancelled out by combining memory bound functions with an automated whitelist. When the caller has fulfilled his “proof of effort” he can be automatically added to the whitelist of the user. This will result in a system where the caller has to only fulfil a “proof of effort” on his first call to the user, the next call will have no delay. As described in the previous section, once this system is known to spammers they could adapt their spam strategy accordingly. This can be solved in the same way as described in section 4.2.1.1 by adding an expiration time for the records on the user’s whitelist. Another option to prevent this is to enlarge the time a caller must spend on his “proof of effort”.

4.2.1.3 Signalling protocol analysis in combination with Whitelisting
To lower the amount of false positives when signalling protocol analysis is used, this technique can be combined with whitelisting. This will allow automated services as in the example of the bookstore described in section 3.1, to be able to call the user, when the user has added this service to his whitelist. According to the authors of [MV05], the addition of a whitelist will provide a low false positive rate.

5. FURTHER RESEARCH
This chapter provides recommendations for further work that needs to be done, to improve spam prevention in VoIP networks.

The main problem most of the VoIP spam prevention techniques face is the ability for spammers to circumvent the technique by just changing his phone number. To prevent this kind of circumvention, research has to be done on how the system of distributing phone numbers can be improved in a way that it will not be that easy to change your telephone number. An improvement of this system will benefit almost all VoIP spam prevention techniques described in chapter 3.

For most of the techniques described in the previous chapters there is no data available about the effectiveness, number of false positives and false negatives in the context of VoIP networks. Research should be done to provide practical test data for each of the technique, so the effectiveness, false positives and false negatives can be compared. This would provide the ability to make a better comparison of the described techniques. For example the paper about signalling protocol analysis provides only theoretical data, research about the effectiveness of signalling protocol analysis in practice is needed to draw a conclusion if this technique will really work.

The handshake/challenge/Turing test technique needs further work on the topic on how to overcome the language barrier when the system is used in an international setting, where people with different languages can call. This is an important topic for this technique, because the acceptance of the technique will partly rely on the language used. There is also research needed for this technique on how to solve the knowledge problem described in section 4.1.2.5, to ensure that no legitimate users are excluded, because they have insufficient knowledge.

6. CONCLUSIONS
The main question that we answer with this research is: “What methods exist against spam over Internet Telephony and which technique or combination of techniques is the most promising for the future?” The following paragraphs present the answer to this question.

The first part of the main research question is answered in chapter 3, eleven methods to protect against spam over Internet Telephony have been identified:

- Signalling protocol analysis
- Do not call register
- Whitelisting
- Blacklisting
- Greylisting
- Rate limiting
- Reputation filtering
• Handshake/Challenge/Turing test
• Payment-at-risk
• Content filtering
• Memory bound functions

The second part of the question, “which technique or combination of techniques is the most promising for the future?”, is answered in chapter 4 by an analysis of the existing techniques with help of the criteria defined in chapter 2. The analysis results in three categories of techniques. Content filtering, do not call registers, reputation filtering, rate limiting and blacklisting are categorized as unsuitable techniques. Whitelisting, signalling protocol analysis, payments-at-risk and greylisting and handshake/challenge/Turing tests are categorized as techniques that have potential. One method is categorized as suitable to use as a spam protection technique in VoIP networks: Memory bound functions. This technique fulfils almost all criteria defined in chapter 2 and is therefore suitable for use.

The combinations of techniques that are suitable for the future are identified in section 4.2. These combinations are: Handshake/challenge/Turing test in combination with whitelisting, memory bound functions in combination with whitelisting and signalling protocol analysis in combination with whitelisting.

So there is not a single technique or combination of techniques that is most promising for the future, but there are several options. Practical information about the effectiveness of the identified suitable techniques and combinations of techniques needs to be researched to identify which of these techniques will be best to use in the future.

VoIP spam protection will probably always stay an arms race between spammers that try to circumvent techniques and researchers that develop new techniques or improve existing, but as shown with a combination of techniques most of the disadvantages can be cancelled out.

REFERENCES


[Har03] Evan Harris. The Next Step in the Spam Control War: Greylisting.


[Hoc05] Sam Hocevar. PWNtcha - captcha decoder

[Sky06] Skype. Skype Help.

Spam, VoIP, Internet telephony, SPIT. 1. Introduction Spam is defined as the transmission of bulk unsolicited emails; it is considered to be one of the biggest problems the Internet has ever faced. With the increasing deployment of Internet telephony solutions, often referred to as Voice over IP (VoIP), it is commonly expected that a similar form of spam will affect this area. This threat is known as SPIT (Spam over Internet Telephony) and it is defined as the transmission of unsolicited calls over Internet telephony.

Details Content analysis cannot be applied to prevent SPIT. The content is very different from email (ASCII text versus coded speech) and voice recognition is not yet fully solved and consuming a lot of computational resources. Background

Definition: The transmission of unsolicited calls over Internet telephony (VoIP) will forge their identities. SPITTING agents capable of placing hundreds of simultaneous automated calls. SIP is not voice only, but applies to Instant Messaging and video as well.

Presentation on theme: “SPAM OVER IP TELEPHONY (SPIT) Identification and prevention Techniques Felipe Santos Manoj Deshpande ECE 4112 Internetwork Security Georgia Institute.”

10 SPIT Prevention Techniques

Pattern/Anomaly Detection Statistical analysis of a user’s VoIP spam or SPIT (spam over Internet telephony) is unsolicited, automatically dialed telephone calls, typically using voice over Internet Protocol (VoIP) technology. VoIP systems, like email and other Internet applications, are susceptible to abuse by malicious parties who initiate unsolicited and unwanted communications, such as telemarketers and prank callers. VoIP calling rates are cheap, and the technology provides convenient, often free tools, such as Asterisk and other applications.