Prepare for VoIP Spam

Baaijens, M.W.

Award date:
2008

EINDHOVEN UNIVERSITY OF TECHNOLOGY (TUE)
Department of Mathematics and Computer Science

and

SWISSCOM AG
Network Development

Prepare for VoIP Spam

by

Mark Baaijens (m.w.baaijens 'at' gmail.com)

"As in many computer security issues, the only way to make sure that you never receive a spam message is to never connect your computer to the Internet. Unfortunately, the unconnected user never receives the many benefits of the most important communications application for business either." [25]

Supervisors:

Bart Jacobs, TUE, Eindhoven, the Netherlands
Robert Muralt, Swisscom AG, Bern, Switzerland

Version 2, 16 November 2007

Preface

From 26 February 2007 until 27 October 2007 I lived in Bern (Switzerland) and worked for Swisscom. During this period I carried out research on VoIP Spam. Due to this research I got an insight into the world of telecommunication and mainly into IP based telephony. This report, which is the main result of this research, serves as my academic thesis to earn the Master of Science degree in Information Security at the Eindhoven University of Technology (TUE).

I thank my supervisors, Robert Muralt (Swisscom) and Bart Jacobs (TUE), for their continual guidance and encouragement and for providing me with critical feedback on my work. Many thanks go to my colleagues at Swisscom, who were very supportive and provided me with knowledge and feedback. Many thanks go to Swisscom as a company, because Swisscom provided me with a work place and the financial means for carrying out my research in Switzerland. Last but not at least, thanks go to Judith (my girlfriend) and my family who stimulated and supported me during the period that I lived in Switzerland.

Mark Baaijens, Bern, November 2007

Abstract

Internet has grown to the modern Wild West where people are annoyed by others without consequences for the annoying party. Due to the openness of the Internet it is very difficult to control the content and its users. One kind of annoyance is Spam, of which E-mail Spam is a well known variety. In this research, Spam is defined as: unsolicited bulk messages aimed at a large public. The Spammer's biggest motivator is, of course, money and the most common method to earn money is joining affiliate programs (see *Section 4.5*).

Since telephony systems are moving to 'all-IP' and IP networks suffer from a trust problem, a lot of threats which apply to an IP network suddenly also apply to telephony, e.g. Spamming. As the use of IP based telephony is growing it is more and more attractive for a new type of Spamming, VoIP Spamming. Since in a VoIP network the costs (i.e. time and money) for the initiator are lower than the costs (i.e. time and money) for the recipient, VoIP Spam is a potential problem. The annoyance level of VoIP Spam is higher than for E-mail Spam, because VoIP communication is pushed by the network (at originator's initiative) instead of pulled from the network (at recipient's initiative). Next to the annoyance for the end user VoIP Spam also causes higher bandwidth demands, higher storage demands, and lower employee productivity.

The audio based and real-time characteristics of VoIP make this technology attractive for Spammers. Because VoIP is audio based and real-time, the most effective filtering techniques for E-mail Spam (i.e. Content Filtering) do not apply directly to VoIP Spam. Thus, VoIP Spam counteraction requires more sophisticated countermeasures in order to increase the Spammer's investment. White/black listing, behaviour analysis, Turing tests, user defined conditions, monitoring, and multiple ID's seem to be promising countermeasures for VoIP Spam counteraction (see *Section 5.1*). Combining multiple countermeasures, dependent on the subscriber's own preference, is the key.

Currently the focus in both literature and anti Spam products is on increasing the Spammer's investment by filtering out Spam messages. Next to increasing the Spammer's investment, decreasing the Spammer's benefits could provide new possibilities. It might be possible to decrease benefits by preventing users from reacting to Spam. For phishing attacks this might be very favourable.

In the coming years telecom providers must start thinking about VoIP Spam and keep this problem in mind while designing new telephony systems. We propose to implement a user portal, strong identity, and monitoring system as described in *Chapter 7*. The user portal gives the user the freedom to configure his telephony service according to his preferences and react on individual VoIP Spam problems. The strong identity is essential for the effectiveness of most countermeasures. A monitoring system is important in order to 'know the enemy' and to anticipate on the evolvement of the VoIP Spam problem.

Illustration: Jack the Spammer

Jack is an IT security specialist at the second largest bank in Europe. He is responsible for the design of security audits in one of the company's head offices in Switzerland. Approximately twice a week he plans an evening for himself in his study, which his wife finds difficult to understand. What he is doing during this time alone is a riddle for everyone who is closely related to Jack. His interest is to keep it like that. Every time someone asks questions about his activities there, he will say that it has to do with keeping up with the current security trends.

Although most people do not know what he is really doing there, we are able to take a look in his 'kitchen'. Two years ago Jack has developed a virus which is able to infect a computer and force it to join in a huge network of infected devices (i.e. a Bot network), which is managed by him. Due to enhancements of this virus, the Bot network currently consists of 20,000 compromised fixed devices and 5,000 mobile devices (connected via wireless Internet access). This Bot network is capable of executing Spam actions via E-mail. In order to make some extra money he has joined several affiliate programs for e-marketing, with which he has made Spam for diet pills and some financial products. Although it is becoming harder to get an order, he definitely avoids sending Spam for sexual oriented or illegal products.

Currently, Jack is looking for a new challenge. The E-mail Spam filters are getting better and therefore it is more difficult to make an effective Spam message. He needs a method to send his message without being bothered by Spam filters. He is currently thinking of using audio-based, and maybe also visual-based, Spam messages in order to bypass the Spam filters and to leave a stronger impression on the recipient. This week he did experiments with audio attachments, which were effective to bypass the Spam filter, but less effective to generate hits…

To be continued…

This story is used as a real case in this report. Throughout this report the story is extended, in order to introduce terms, ideas and concepts which are used in the subsequent text.

Table of Contents

Chapter 1
Introduction

Walking from platform 13 into the tunnel one joins a crowd of people, who are going through to enter the main hall of Bern Central Station. In the tunnel one passes four 1,5mx3m-billboards, twelve 2mx1m-billboards and two display windows. The main hall is the central point of the train station. Apart from the timetable, there are another four 2mx1m-billboards and two 3mx4m-screens, which sometimes make you think the light is flashing. Very often you pass one ore more persons who give you a flyer or a sample product. As soon as you are outside the building you have passed by 75 m^2 of advertisements and you have one or more flyers in your hand.

The amount of advertisements people are confronted with in everyday life, seems to bother nobody, although this is a lot. In contrast, E-mail advertisements (generally called Spam), annoys people. Off course, the main difference here is that bill boards are dedicated communication channels for advertisements, and E-mail is not. A communication channel on which you get both personal messages and advertisements requires work in order to pick out the personal messages (i.e. relevant communications) and ignore advertisements (i.e. irrelevant communication). Communication channels which are cheap, widely used, and ready for automation are most susceptible to Spam.

Since Spam (distribution of unsolicited bulk messages) is already a big problem, almost everybody is nowadays familiar with the fact that Spam is a burden and a hindrance to us. Although a lot of people correlate Spam with E-mail, Spam also occurs in combination with other communication methods, for instance, Instant Messaging or Voice over Internet Protocol (VoIP). Spam in combination with VoIP (e.g. Internet Telephony) is a form of unwanted communication and is expected to become an issue in the near future because it may be computer generated like E-mail Spam [2][28][29]. By the time that VoIP is widely used it will satisfy all conditions to be susceptible to Spam. In literature VoIP Spam is also called SPIT (Spam via Internet Telephony) or Vamming (VoIP Spamming), but in this document the term VoIP Spam is used.

VoIP Spam differs radically from E-mail Spam and therefore countermeasures for E-mail Spam cannot be used directly. More advanced techniques are needed in order to fight it. For instance, content filtering cannot be used in case of VoIP Spam because the aim is to identify a Spam call even before the phone is ringing (i.e. before there is any content available).

Due to the fact that VoIP is a fast upcoming technology and countermeasures for VoIP Spam are difficult to design, research is needed on the VoIP Spam phenomenon. By means of this research we want to disclose the unique characteristics of VoIP Spam and

define and evaluate countermeasures. The objective of this research is to have a clear view where there is a risk and how to deal with VoIP Spam in specific cases. The central question therefore is: **How can VoIP Spam be kept under control?** The research is done under the auspices of Swisscom AG, which we will refer to as Swisscom. Swisscom, which is a Swiss telecom provider, offers two VoIP products on the Swiss market (namely a residential [30] and an SME product [31]) and therefore is interested in this research.

It is debatable whether it is not too early to carry out a research on VoIP Spam because the impact VoIP Spam is still very low. However, it is better to be one step ahead from the attackers than the other way around. Since new IP based telephony systems are being built, this is the right moment to investigate VoIP Spam. By means of this research, techniques that will counteract Spam could be implemented in an early design phase.

This research report is organized as follows: *Chapter 2* gives the scope and the main objectives of this report. *Chapter 3* defines the basic terminology used. *Chapter 4* contains a problem analysis. *Chapter 5* describes a number of theoretical countermeasures to counteract VoIP Spam. *Chapter 6* describes anti VoIP Spam products which are available today and describes the evaluation of three of these products. *Chapter 7* designs novel countermeasures for a telecom provider. *Chapter 8* contains recommendations for telecom providers and for anyone else who wants to counteract VoIP Spam. *Chapter 9* indicates related work. *Chapter 10* points out some issues which could be the subject of further research. *Chapter 11* gives the conclusion.

For this research a questionnaire has been used to gather people's thoughts and expectations about VoIP Spam. The questionnaire respondents have different backgrounds in the field of telecommunication. Most of the respondents work for Swisscom, but others work for VoIP suppliers or telecom regulators. The result of this questionnaire is placed in *Appendix A*.

1.1. Conventions

Whenever questionnaire feedback is used in this document, one of the following references is used:

- **[Q `<question>`]** − A reference to a specific question. `<question>` stands for the question number. For example, for a reference to question 2.3 of the questionnaire [Q 2.3] is used.
- **[Q `<question>/<respondent_id>`]** − A reference to a specific answer. `<question>` and `<respondent_id>` stand for the question number and the id of the respondent respectively. For example, for a reference to the answer of respondent 3 on question 2.1 the reference [Q 2.1/3] is used.

Chapter 2
Scope and Objectives

The aim of this research is to disclose the unique characteristics of VoIP Spam and define and evaluate countermeasures. This research does not attempt to be a deep study of anyone of the countermeasures, but it aims to be more generic. Defining countermeasures should be preceded by unravelling the actual problem. This is done by means of a problem analysis, which will give an overview of the important issues regarding VoIP Spam.

This research is done under auspices of Swisscom, which is the Swiss main telecom provider and offers VoIP services on the Swiss market. Telecom providers play an important role in the counteraction of VoIP Spam. Swisscom is therefore interested in this research and provided resources to carry it out. Swisscom is also a favourable environment for this research because this environment provides knowledge and expertise on VoIP technologies. Furthermore, there is a VoIP test infrastructure available, which has been used to do experiments with VoIP Spam and evaluate countermeasures. Although this report is written from a telecom provider's point of view, the aim is to have a generic approach for VoIP Spam counteraction.

This report is the outcome of the VoIP Spam research and its aim is to provide an insight into the VoIP problem to a broad audience. The most parts of this report are intended to be readable for non-technical readers. Besides this report, the document 'Research Documentation' is delivered, which is a more detailed document about the research. This document is meant to serve technical readers who are interested in the details of the research process and a technical description of the tools used. The research documentation document is, however, confidential and only for use within Swisscom. It is not part of this master thesis

Currently, the definition of Spam is ambiguous, but a clear definition of Spam is essential for a research on this topic. In *Section 3.1* the term Spam is defined to be 'unsolicited bulk messages aimed at a large public', consequently this research is about unsolicited communication which is sent in large volumes. Since the main focus of this research is on telephony via an IP based network rather than via the traditional telephone systems, the terms Telephone Spam and Call Spam are too general to serve as subject of this report. Therefore, this report is about VoIP Spam, which is actually Telephone Spam via an IP network. Although there are a lot of different types of Spam possible in a VoIP network, the main focus is on Spam via IP based telephone calls. *Section 3.3* describes the term VoIP Spam in more detail.

There are multiple important VoIP protocols available today to set up a phone call. The Session Initiation Protocol (SIP), explained in *Section 3.2.3*, is chosen to be used in this research. This decision is twofold: (1) SIP is dominating the VoIP market and also Swisscom has made an explicit decision for SIP; (2) SIP is used for new telephony systems (e.g. SIP is selected by the standards body 3rd Generation Partnership Project (3GPP) to be the protocol for IP Multimedia System (IMS) [10]). Although there is an explicit choice for the SIP protocol in this research, this has no serious consequences for the outcome of this research. Neither VoIP Spam nor the counteraction does depend on the selected protocol. However, it is possible that the implementation of the countermeasures depends slightly on the selected signalling protocol.

VoIP Spam phone calls could originate and terminate in networks other than IP networks, but for simplicity reasons we focus in this report only on phone calls originated and terminated in a VoIP network. This has no serious consequences for the prevention of VoIP Spam, though. It is, however, still an important question whether Spam prevention on the transit network is the responsibility of the network provider.

It is possible to hijack a multimedia session and inject a Spam message in a legitimate telephone conversation. Although this is also a form of Spam, it is outside the scope of this document because here connection security is the underlying issue.

The information provided in this report is obtained mainly by means of literature study, a questionnaire (*Appendix A*), and a SPIT Analysis Platform (*Appendix B*), which has been set up to evaluate spam methods and countermeasures. Since VoIP Spam is a very new concept at the time of writing, there is limited scientific literature available. Therefore, literature from related fields (e.g. E-mail Spam) and non-scientific literature is also used in this research.

Chapter 3 Terminology

***Illustration**: Currently a VoIP network is being implemented at Jack's office. The aim is to replace the old and expensive ISDN PBX's with new and cheaper IP PBX's. Jack's role in this project is to identify the security threats for this new technology. He is going through a list of security threats in IP networks in order to check the applicability on VoIP. Due to this list he starts to think about VoIP Spam and searches the Internet for literature in this field. While he is researching this topic, the idea comes up to use it for extending his own Spam activities.*

The same evening he goes to his study to find out more about VoIP Spam and to identify his capabilities of making it. He registers for some free VoIP accounts and installs an open source IP PBX in order to do some experiments.

To be continued…

The aim of this section is to describe the basic terminology for this report; all other terminology will be explained at its first usage. Since not all terms have a well-defined meaning, it is for some of the terms necessary to create our own definition.

3.1. What is Spam

Although most people are familiar with the term Spam, the definition of Spam is currently not evident. Some people correlate Spam with E-mail, but for others the term Spam is more generic and could also apply to other communication methods. As can be seen from *Table 1*, different sources define Spam differently.

Of course, the definitions provided in *Table 1* are important, but for telecom providers the telecom authority's definition takes precedence.

BAKOM, which is the Swiss telecom authority, defines Spam in the following way:
"Spam is an electronic message, which is sent automatically to multiple recipients without their consent." [Q 1.1/29]

OPTA, which is the Dutch telecom authority and very active in the field of Spam prevention, bases their definition on the Dutch law [12] (Article 11.7 of the Dutch law for

telecommunication). This law defines Spam as "unsolicited communication for commercial, ideological, or philanthropic purposes, initiated by a machine and without a relation between the originator and recipient".

Source	Definition of 'Spam'
MacMillan English Dictionary [3]	Emails that are sent to large number of people on the Internet, especially when these are not wanted.
English Wikipedia [4]	Unsolicited bulk messages, which are universally undesired.
Dutch Wikipedia [5]	Unsolicited E-mail which is sent in large volumes.
German Wikipedia [6]	Unsolicited, electronic messages which are unwanted and sent in large volumes, or contain commercial content.
Britanica Encyclopedia [7]	Unsolicited advertisements for products and services.
Britanica Student Encyclopedia [8]	Unsolicited Bulk Commercial E-mail.
IETF Internet Draft: The Session Initiation Protocol and Spam [1]	Bulk unsolicited messages.

Table 1: Different sources and their definition of Spam

It would be fair to use the intersection of all definitions listed before, which will result in a simple and clear definition for Spam, namely 'unsolicited messages'. This is already a good definition. However, by using this definition we should also classify the love letter from your love as Spam because normally you did not ask for this. It should be postulated that Spam only occurs in large volumes and that Spam has a large target group. As a result, Spam is defined here as **'unsolicited bulk messages aimed at a large public'** and this definition is very similar to the definition of BAKOM and OPTA.

Spam is used in various ways:

- Spam is the verb describing the action of sending unsolicited bulk messages (i.e. to spam = to distribute unsolicited bulk messages to a large public).
- Spam is the uncountable noun describing the end-product of spamming behaviour (i.e. spam = unsolicited bulk message aimed at a large public).
- Spam is the uncountable noun describing the phenomenon of sending unsolicited bulk messages (i.e. Spam = distribution of unsolicited bulk messages to a large public).
- The originator of Spam is defined as the Spammer.

It is important to notice that in principle there is no relation between the originator and the recipient of Spam, the Spam message is not personal and for the Spammer quantity is more important than quality. Since the definition of Spam which is stated above still can

be unclear, it is useful to put it within a framework and include and exclude some concepts.

- **DoS (excluded)** − Although some definitions of Spam seem to be applicable to Denial of Service (DoS) attacks, this is not included. The important difference between DoS and Spam is that the aim of Spam is to reach a large number of people and the aim of DoS is to destroy a service [2]. For Spam it is essential that the receiving side remains up and running.
- **Chain Letters (included)** − Sometimes normal users are persuaded to Spam by means of chain letters. Since the originator of such a chain letter (i.e. the Spammer) wants his message to be sent to a large public, this concept is included in the term Spam.
- **Stalking (excluded)** − Stalking is also a form of unsolicited communication, but is not classified as Spamming. Although stalking could be very annoying and intimidating, the focus is on one individual whereas the focus of Spam is on multiple individuals and very likely as many people as the Spammer can reach.

Some people use the term Ham to identify legitimate messages (i.e. Ham is the opposite of Spam), but in this report this term is avoided. Legitimate call behaviour is our presumption.

Opt-in and opt-out are terms which are used in combination with Spam [47]. In the context of Spam opt-in means ‘choosing to receive a certain type of unsolicited communication’; opt-out means ‘choosing to not take part (anymore) in receiving a certain type of unsolicited communication’. Opt-in and opt-out can be seen as subscribe and unsubscribe, respectively.

Spam needs a communication channel and in theory Spam could occur on every communication channel. Whether a communication channel is attractive for Spamming behaviour depends highly on the characteristics of that channel, e.g. the size of the community, the costs to use the channel, the openness of the channel, etc. In practice most Spam occurs on communication channels which are based on the Internet Protocol (IP) (e.g. E-mail, IP based telephony, Instant Messaging), due to the attractive characteristics of IP based communication. In this report the focus is on Spam via IP based telephony and before going into the details of this concept it is important to have a clear understanding of the VoIP technology.

3.2. What is VoIP

The term VoIP (Voice over IP) is used for telephony on an IP based network. The relatively new concept of VoIP can lead to cost savings, because for both voice and data only one network is needed. Since very often Internet access is flat-rate based now telephony could also become flat-rate based. Another advantage of VoIP is that it could also easily be combined with other kind of IP-based services. VoIP is not the same as

Internet Telephony, but the terms VoIP and Internet Telephony are very often interchanged. Although the telephony network is very often the Internet, VoIP has a more generic meaning than Internet Telephony. VoIP could also occur on a corporate LAN rather than on the Internet.

3.2.1. The transition to all-IP

The current trend in telephony business is a change from the Public Switched Telephone Network (PSTN, see *Section 3.4*) which is a circuit-switched network, into a packet-switched telephony network which is based on the Internet Protocol (IP). Next Generation Networking (NGN) is more and more seen as the successor of the current PSTN. One example of an NGN network is IP Multimedia Subsystem (IMS), which is the 3GPP's architectural description of an IP based multimedia network. Currently Swisscom is building an IMS in order to have a future proof, flexible, IP based, telephony network.

Currently, most phone calls are still done via the PSTN, but the use of VoIP is increasing fast. In traditional telephone systems the end-devices are relatively 'dumb' and the intelligence is in the network. The IP network, instead, is 'stupid' and the focus is on transport of packets, regardless what the content of this packet is [17]. As a result, it is relatively easy to integrate new services. VoIP makes it possible to integrate multiple communication methods. For instance, spelling your name during a telephone conversation will be unnecessary, because sending the correct spelling is possible via Instant Messaging, which is an integrated feature on your communication device.

The most important reason why most people and enterprises switch from traditional telephony to VoIP telephony is that VoIP is 'cheaper' [39]. Although the lack of hard evidence of communication via an IP network being cheaper than communication via the PSTN, it is generally assumed that the following aspects enable some cost-savings:

- The already existing IP based data network is now also used for telephony. As a result there is only one network for both data and voice.
- Hardware in the PSTN is more specialized and thereby more expensive than hardware for IP networks.
- In a packet switched network (e.g. The Internet) the physical network is used more efficiently compared to a circuit switched network (e.g. the PSTN) [17].

On the other hand, IP based communication has some problems like every new technology has. A packet switched network is more vulnerable to delay, due to the unpredictable path the packets are following and the first-come-first-serve principle. The network relays the packets on best-effort basis and there is no guaranty how good 'best-effort' is. Since every packet's content is treated equally, it is impossible to identify services which require a more 'stable' connection (i.e. higher Quality of Service). Next to the Quality of Service (QoS) problem, there is also a trust problem in IP networks, which enables misuses such as Spam.

3.2.2. Network Architectures for VoIP

There are roughly two types of network architectures for VoIP networks:

- A decentralized VoIP network (*Figure 1*) where all users potentially can connect to every other user (assuming the address is known) and all network entities have the same role. This architecture, which is based on the peer-to-peer model, will result in an open environment in which trust in the other users (peers) is important, since there is no central control. In this network type Spam could only be counteracted at the terminating side (i.e. side of the callee).
- A centralized VoIP network (*Figure 2*) where all users are connected to each other via a central network, owned by the service provider. This architecture, which is based on the client-server model, will result in a controlled environment in which the trust in the service provider is important. Since this report is written from a VoIP service provider's point of view, the focus is on a centralized network for VoIP. In this network type Spam countermeasures could be placed in the network itself.

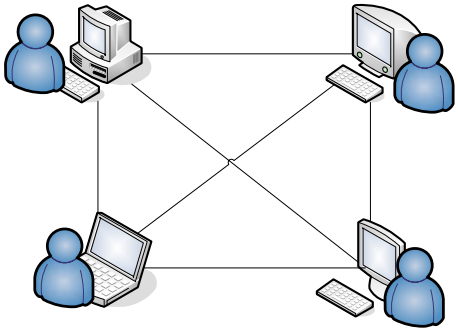

Figure 1: Peer-to-peer architecture

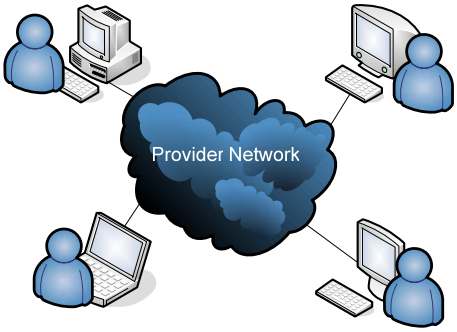

Figure 2: Client-server architecture

3.2.3. The Protocols

A VoIP phone call consists of two parts: the signalling part and the media part. The signalling part is for establishing the phone call and an agreement on the used method (e.g. the media codec). The media part is for transmitting the actual voice packets (i.e. the payload). For both parts there are multiple protocols available.

For the signalling part there are currently two important open standards available, Session Initiation Protocol (SIP), specified in [13], and H.323, specified in [14]. SIP, which is an IETF standard, is a simple signalling protocol designed for IP based multimedia communication. H.323, which is an ITU standard, is an umbrella term to identify multiple protocols for audio and video communication.

Next to these standards there is also Skype, which is a very popular VoIP technique (in 2006 4.4% of international IP traffic was via Skype [15]). In contrast to SIP and H.323, Skype is not an open standard. The Skype program is closed source and due to code

obfuscation Skype attempts to make it impossible to reverse engineer the program. Despite the popularity of Skype, it is not a simple replacement for the normal telephone connection because it is only possible to phone via a dedicated soft phone (The Skype program) or hardware which is seldom compatible with other networks and techniques. It is difficult to have direct interconnection between the Skype network and VoIP networks based on other protocols.

In this research there is an explicit choice for SIP, because in the research environment at Swisscom, SIP is chosen to be the standard. SIP is a text based protocol like HTTP and SMTP, and a SIP message is either a Request (*Table 2*) or a Response (*Table 3*). In the basic specification of SIP (i.e. RFC 3261), there are six different Requests (i.e. REGISTER, INVITE, ACK, BYE, OPTION, and CANCEL), which can be used to initiate, modify and terminate sessions. The Response, which is a reaction on the Request, contains a three-digit status number, saying what the status of the request is.

SIP Request	Description
REGISTER	Registers a client to a SIP server
INVITE	Invites a user for participating in a multimedia session
ACK	Confirms that the final response from the INVITE is received
BYE	Terminates the multimedia session. Can be send by every participator in the multimedia session
OPTION	Queries the capabilities of the server
CANCEL	Cancels any pending requests, but does not terminate any accepted session

Table 2: SIP Requests

SIP Response	Description	Examples
1xx	Informational Responses	100 Trying, 180 Ringing
2xx	Successful Responses	200 OK
3xx	Redirection Responses	302 Moved Temporarily, 305 Use Proxy
4xx	Method Failure Responses	401 Unauthorized, 404 Not Found
5xx	Server Failure Responses	500 Server Internal Error, 502 Bad Gateway
6xx	Global Failure Responses	600 Busy Everywhere

Table 3: SIP Responses

A SIP-based VoIP network consists of multiple entities of which the User Agent, Proxy Server and the Register Server are the most important ones. *Figure 3* shows a simple example of SIP communication.

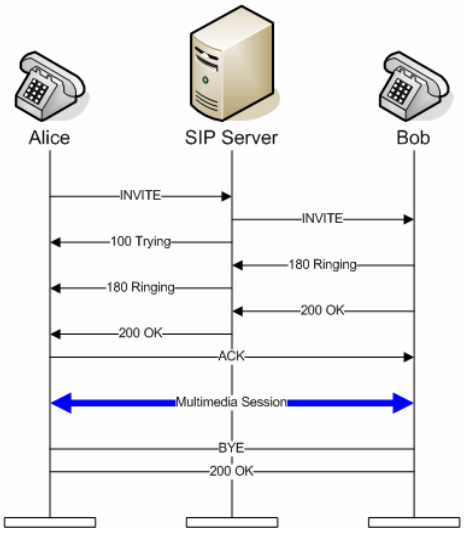

Figure 3: SIP signalling

The Session Description Protocol (SDP), specified in [59], is carried by the SIP Requests. SDP describes the media part of the voice call (e.g. the audio codec, the IP ports that are used, etc.). Very often media transport is done by means of the Real-time Transport Protocol (RTP), specified in [60]. RTP is a standardized protocol for delivery of audio and video streams. *Figure 4* shows a schematic overview of all protocols involved in a SIP based phone call. As can be seen from this diagram SIP can be used in combination with both the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), but in most cases SIP is used in combination with UDP.

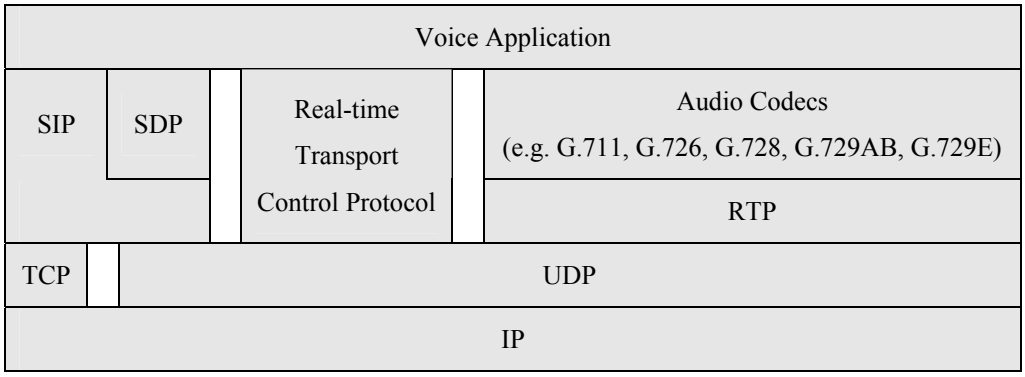

Figure 4: Protocol stack SIP based telephony

3.2.4. Public User Identities

In any type of network there must be a way to uniquely identify users in order to communicate with a specific user. In the PSTN we are used to a telephone number, which is in fact an ordered sequence of digits. In the PSTN, the length of a telephone number that is used by the caller to contact the callee depends on the geographical distance between the originating side and the receiving side (i.e. within the same area, another region or another country).

In VoIP, a Public User Identity is expressed in a SIP Unified Resource Identifier (SIP URI) [10]. A URI is a string, which is of the form `<scheme>:<resource>`. For example, an HTTP URI can be `http://www.swisscom.com` where `http` is the used scheme and `//www.swisscom.com` is the resource. For a lot of protocols there is a standardized URI definition. A SIP URI is defined to have the following format:

```
SIP:<user>@<domain>:<port>;<parameters>
```

- **`<user>`** − The identifier for the specific user. This could be a name, a (telephone) number, or another string identifying the user.
- **`<domain>`** − The hostname or IP-address of the domain where the user is known. E.g. the domain name of the service provider.
- **`<port>`** − The port number where the request is to be sent. This field is optional and the default value is 5060 (i.e. the default SIP port).
- **`<parameters>`** − This optional field enables the opportunity to give extra information.

Table 4 shows some different types of SIP URI's that are possible. From this list Type I and Type II are the ones that are used most frequently. If the VoIP Network has interconnection to the PSTN, (at least) the Type II SIP URI must be used, because traditional telephones are only able to dial digits.

Type I:	Format: `SIP:<user>@<domain>` Example: `SIP:Alice@bluewin.ch`
Type II:	Format: `SIP:<number>@<domain>;user=phone` Example: `SIP:+41485001000@bluewin.ch;user=phone`
Type III:	Format: `SIP:<IP-Address>` Example: `SIP:192.168.1.41`

Table 4: Common SIP URI types

The Telephone Numbering Mapping (ENUM), specified in [61], is a DNS-based technique for resolving SIP URI's from telephone numbers. Therefore the telephone number (in international format) is translated into a E.164 format for which the digits are put in reverse order with a dot between every two digits and '.e164.arpa' in the end. For instance, the telephone number +31 118 714025 is translated into 5.2.0.4.1.7.8.1.1.1.3.e164.arpa. The resulting DNS query can be used to get the Naming Authority PoinTeR (NAPTR) record, specified in [62]. In this record user information is stored, e.g. SIP address, E-mail address.

Authentication

In digital communication, authentication is the process of verifying the (digital) identity of the user. In order to determine a caller's identity, authentication is required for telephony. In the PSTN, authentication is done by means of the physical line. Since VoIP enables users to be nomadic there is a need for a different method of authentication. Currently in most implementations of SIP, authentication is done by means of the digest access authentication, specified in [63]. Digest access authentication is a challenge-response authentication mechanism which is based on the MD5 hash algorithm.

In this report we use the notion of 'strong identity' to express the quality of the authentication. A strong identity means both that it is difficult to spoof the identity and that it is difficult to obtain a fresh identity. The first condition is dependent on the quality of the authentication technique and the strength of the secret involved (i.e. password or key). The latter condition is in many cases fulfilled by the fact that a subscriber has to sign a contract with the telecom provider for which he has to show his passport (or a copy).

In cellular telecommunication a Subscriber Identity Module (SIM), which is an application on a removable smart card and contains the user's private key, is used in order to authenticate. A user is only able to phone with the device containing the SIM-card. For the authentication in SIP the secret is stored in the brain of the user rather than stored on a SIM-card. In a SIP VoIP network, where (only) a username and password is required to register a phone, it is possible to register multiple devices for the same SIP URI.

3.2.5. Stakeholders

In a VoIP network there are different stakeholders, which all have their own requirements and expectations regarding the VoIP system:

- **End-user** − The most important stakeholder is the end-user who uses a soft phone (i.e. software to make phone calls) or an IP phone (i.e. device to make phone calls) to communicate. The originator of a phone call is the caller and the recipient is the callee.
- **Provider** − Although it is possible for end-users to communicate directly to each other, often the communication is done by means of a service provider's VoIP service, for which the network provider's network is used. The service provider and the network provider are also important stakeholders for VoIP.
- **Spammer** − In this report we identify another stakeholder, the Spammer. Since his interest is to distribute a message and a VoIP network provides attractive possibilities for Spamming, he is interested in the VoIP system too.

3.3. What is VoIP Spam

In *Section 3.1* Spam is defined as 'distribution of unsolicited bulk messages to a large public'. VoIP Spam, which is a yet non-existing problem, is obviously defined as '**distribution of unsolicited bulk messages to a large public using a VoIP network**'. The focus in this report is on Spam via VoIP telephone calls, which is often done by means of automated machine calls playing an audio message to the recipient.

In some literature the term SPIT (Spam over Internet Telephony) is used instead of VoIP Spam, but according to our opinion the term VoIP Spam is more general. We will try to use VoIP Spam consistently in this report. The term SPIT occurs a couple of times though, because Swisscom and other commercial companies use this term.

Whether a call is Spam or not is not always clear; it depends highly on the end-user's opinion. Some people like to get questionnaire calls (there are even people who enjoy giving wrong answers), but for others these calls are very annoying. Although this uncertainty makes it difficult to distinguish between legitimate use and Spam, we use the term VoIP Spam in this report for all VoIP calls that are unsolicited by universal belief.

Chapter 4 contains a more thorough description of VoIP Spam.

3.4. Telecom Related Terms

Since this research is done in the field of telecommunication, some telecom-related terms are used. These terms are shown in *Table 5*.

Term	Description
Caller / Originator	The user who is initiating the call (could be a person or a machine)
Callee / Recipient	The user who is receiving the call (could be a person or a machine)
Network Provider	In telephony a Network Provider is the entity which owns the telephony network. The use of this network is sold as a service to other entities.
Service Provider	In telephony a Service Provider is the entity which enables the telephony services for the user. In practice the user has a contract with a Service Provider. A Service Provider uses the network of the Network Provider to enable the services. Both the Network Provider and the Service Provider could be the same company.
PSTN	Public Switched Telephony Network – The traditional telephony network which is circuit switched instead of packet switched, like an IP-network.

PBX	Private Branch eXchange - A telephone centre which can handle calls to extensions (local end point) and to trunk lines (i.e. connections to other telephony networks).
IVR	Interactive Voice Response (IVR) is a technique for machines to detect voices and touch tones. IVR is for example used to navigate through menus when phoning with a large company.
Premium rate phone number	In telephony a premium rate phone number is a number which has a special rate. Usually part of this the call charge is paid to the service provider and the other part is paid to owner of the premium rate phone number. These numbers could be used for providing special services for support or entertainment.
Call Forking	In (VoIP) telephony call forking is the ability to receive a phone call on multiple end-devices. As a result a phone call could be received at multiple geographical locations in parallel or sequentially.
Lawful Interception	Lawful interception (wiretapping) is interception of telecommunication (content) in cases that are officially demanded by the government or another authority.

Table 5: Telecom related terms

3.5. Security Related Terms

Since security is an important issue in this report, some security-related terms are used. These terms are shown in *Table 6*.

Term	**Description**
Confidentiality	Secrecy of information
Integrity	The quality of a system or information being in a good condition, i.e. without any damage or mistakes.
Availability	The degree in which a system is in a committable state in order to use it properly
False Positive	A malicious user who is accepted by the system
False Accept Rate	The proportion of False Positives
False Negative	A legitimate user who is rejected by the system
False Reject Rate	The proportion of False Negatives
Bot network / Zombie network	A (virtual) network of infected devices which are under control of one person and able to perform actions like Spamming (see *Section 4.6.3*)

Onion Routing	A cryptographic method to hide the origin of a data packet by transporting it via a random and undisclosed path to its destination. The aim of Onion Routing is to disable back tracking (see *Section 4.6.3*).

Table 6: Security related terms

Chapter 4
Problem Analysis

***Illustration**: After some days of doing experiments with VoIP Spam, Jack contacts his affiliate partners in order to propose his new Spamming method. One partner is interested in Spam via VoIP calls and delivers an audio message containing 10 seconds of product advertisement for cheap imitation Rolex watches.*

At his work he discusses the VoIP Spam topic with some legal experts. As a result, he get an insight into the legal possibilities for VoIP Spam. He finds out that the law is not completely clear about machine generated phone calls.

Jack configures one of his old PC's to produce VoIP Spam. In order to do so he installs IP PPX software and designs software to make multiple calls and play the audio message. He decides to start with a simple Spam action, for which he uses a Swiss VoIP network. For this network his account number only consist of 6 digits. When he registers for another account at the same provider he observes that this account number is just the other account number increased by one. Thus, for him the easiest way to obtain valid account numbers for Spamming is just to count down starting at his first account number. He implements a count down function on his Spam machine. For his first Spam action, he configures his Spam machine to make two calls in parallel. Once everything is configured he executes his action at Friday 17:00. His machine reaches account 000000 some minutes after 21:00.

When Jack's Spam machine is finished he evaluates the action. One third of the people who were online took the call and listened to it for an average of 5 seconds. He has configured his Spam machine to deal with the voicemail service of this VoIP provider, so the Spam calls have terminated in the voicemail boxes of the user who were not online. Since this VoIP provider forwards voicemails to E-mail, the offline user have received the Spam message in their E-mail inbox.

To be continued…

The aim of this chapter is to unravel the phenomenon of VoIP Spam and to indicate the actual problem. Furthermore, this chapter takes a look at the Spammer and his methods, describes the impact of VoIP Spam, and discusses some important issues regarding VoIP Spam. Although the main focus is on VoIP Spam, many parts of this chapter are also applicable to other types of Spam.

4.1. Communication and VoIP Spam

Communication has always been important to share information and to maintain social relationships. There are roughly two types of communication; (1) Broadcast methods, which are usually meant for monologue communication; and (2) Unicast methods, which are usually meant for dialogue communication. In case of broadcast communication messages are usually pulled from the network (at recipient's initiative) and in case of unicast communication messages are pushed by the network (at originator's initiative). VoIP Spam can be seen as the misuse of a unicast communication method for broad dissemination of information.

For the analysis of the VoIP Spam problems two concepts are important to pay attention to: telecommunication and unsolicited communication.

4.1.1. Telecommunication

For a very long time the challenge to have long distance communication (i.e. telecommunication) has fascinated people. There are very old experiments with telecommunication (i.e. smoke signals, drums, semaphores), but nowadays almost every telecommunication system uses electro magnetic waves or optical fibre to transmit signals. The main challenge is to improve the amount of signals that can be sent (reliably and securely) within the same timeframe (i.e. bandwidth).

Modern telecommunication methods have become very important for the world society. Especially telephony is a popular method for communication. The concept of telephony, which has existed for more than hundred years, makes many governments, enterprises and people depending on it. As a result, it is important that a telephony system is reliable. Unreliable telephony would cause less profit for companies whose business model depends on the telephony system (i.e. pizza deliverers, call centres).

In the end of the 20th century the world embraced another telecommunication method, the Internet, which makes people even more depending on it. Currently on almost every office desk a computer with high speed Internet access has been placed next to the telephone.

The Internet is based on the Internet Protocol (IP), specified in [80]. Since the focus in an IP network is mainly on the transport of data, it is relatively easy to develop new application running on this network. As a result, an IP network is an open network, meaning that the intelligence is not in the network but at the edge of the network. Although the Internet gave the world more possibilities to share information and to communicate, the openness of this network can be a threat. Due to the openness of the Internet there is a trust problem, and therefore information security became essential.

The current trend is that telephony systems and the Internet are merging together and therefore all security threats which apply to the Internet suddenly also apply to telephony. Spam is one example of such a threat.

4.1.2. Unsolicited Communication

The reliability of a communication method depends on many factors. One factor is the degree of control recipients have on the communication channel. It is impossible to eliminate all unsolicited communication, but it is favourable that recipients have at least the opportunity to finish communication in case there is no interest. When a recipient does not like the program on the television he can switch to another channel, or just walk away in case there are family members involved. However, Spam is a somewhat more difficult problem to walk away from.

Not all unsolicited bulk communication can be classified as Spam. The question whether communication is Spam or not depends highly on the working method of the originator and the opinion of the recipient. Another important issue is whether or not there is a relation between the originator and the recipient. If the recipient has agreed with receiving 'unsolicited communication' from this originator, it is not classified as Spam.

4.2. Characteristics of (VoIP) Spam

By the definition of Spam in *Section 3.1*, Spam is sent in large volumes and as a result the recipient is not treated personally. Since there is no relation between the Spammer and the recipient, the Spammer does not know its victims and the victims do not know the Spammer. A Spammer initiates a lot of calls, but (almost) nobody initiates calls to him. Furthermore, the communication is very likely to be one-way; the originator sends a message, but there is little response from the recipient.

The Spammer uses his bandwidth optimally, thus there is a constant stream of calls coming from him. However, the statistical distance between spam and legitimate behaviour can be very small [Q 2.7/31]. For example, a call centre is also interested in using its resources optimally.

It is likely that products in Spam advertisements have a lack of quality, because Spammers use an illegal and cheap way to advertise. There are confirmed cases of people who died of using cheap medicines due to Spam advertisements [75].

The next section describes more characteristics of VoIP Spam by means of a comparison with E-mail Spam.

4.3. VoIP Spam vs. E-mail Spam

Like we all know E-mail Spam is a current problem (in August 2007 74% of E-mail messages worldwide was Spam [64]). To predict the evaluation of the VoIP Spam problem we could look at the development E-mail Spam has made and still is making. It is likely that Spammers, who are Spamming via E-mail today, will spam via VoIP tomorrow. Both E-mail Spam and VoIP Spam are, due to flat rates on internet access,

cheap and therefore attractive. There are some differences between these two phenomena, which we have to keep in mind when predicting the trend of VoIP Spam.

E-mail is a text based medium in which the user has to pull the messages (i.e. download the message). In contrast, VoIP is audio-based instead of text-based. Therefore, the most successful countermeasure for E-mail Spam, i.e. content analysis, is more difficult to implement for VoIP Spam (*Section 5.1.6*). Furthermore, VoIP is a real-time medium in which the messages are pushed (i.e. the phone rings without asking). The real-time characteristic makes VoIP Spam even more annoying than E-mail Spam already is.

Of course, a different medium implies different communication protocols, which are the Simple Mail Transfer Protocol (SMTP) for E-mail and SIP for VoIP. The original SMTP standard did not support authorization, although there are some techniques to build authentication into SMTP (i.e. TLS, SMTP-AUTH, S/MIME). Most implementations of SIP are equipped with a challenge-response authentication mechanism. Since the lack of SMTP authentication was one of the reasons for the current amount of E-mail Spam, this might be slightly different for VoIP Spam.

VoIP Spam can also be more effective than E-mail Spam, because audio leaves a stronger impression than text. Furthermore, a recipient can choose the speed he looks at text, but he cannot choose the speed in which an audio message is 'played' to him. You can ignore a Spam E-mail, but it is more difficult to ignore a Spam call.

Since the Internet is full of services for which registration is obligatory before using it, one's e-mail address, which is very often used to validate these registrations, ends up in a lot of databases. Due to the amount of unreliable database owners and security problems, these databases are an attractive source for gathering E-mail addresses for Spamming. Although this is not the case for telephone numbers, in the telephony world there exists a public telephone directory which is a list of alphabetically and geographically ordered user ID's, ready to use for Spammers. In VoIP there is the ENUM system (*Section 3.2.4*), which is an attractive resource for gathering user information.

VoIP Spam	**E-mail Spam**
• Audio based: *Difficult to perform content analysis. *Disables quick Spam identification.	• Text based: *Relatively easy to analyse content. *Enables quick Spam identification.
• Messages are pushed by the network (real-time medium).	• Messages are pulled from the network.
• Public telephony directory is a huge repository of telephone numbers.	• E-mail address is often used for account validation.
• Standard authentication.	• Weak authentication.

Table 7: VoIP Spam vs. E-mail Spam

Table 7 shows a summary of the differences between VoIP Spam and E-mail Spam. To conclude this comparison: VoIP Spam is more difficult to counteract than E-mail Spam and the level of intrusion is higher.

4.4. The Cause of (VoIP) Spam

Like we mentioned earlier in this report, there are a couple of conditions which makes a communication method vulnerable for Spam:

- Low or flat rated communication
- Open network which is ready for automation
- Large user community

The first two conditions are fulfilled by any IP based network and the last condition is more dependent on the user acceptance of the specific communication method. For VoIP, only the last condition has not yet been (sufficiently) reached to make it a problem. As soon as the VoIP user community is large enough VoIP Spam could become a problem. What the exact threshold is for this problem is hard to say.

If we analyse the three Spam enabling conditions, we see that they are all related to costs and efforts. If these conditions are fulfilled, the costs for broadcasting messages are low enough to make Spamming attractive. In this case Spam is much cheaper than employing a call centre with human call agents. For the recipient, Spam is most probably more costly in terms of time and annoyance. According to our opinion, the real problem of Spam is that the originating costs are lower than the receiving costs.

Since VoIP communication is audio-based, the potential Spammer could express more creativity while making the message. This could make VoIP Spam attractive and more difficult to filter.

Not so long ago every self-respecting company, whose intention was to sell products, was interested in building a positive image. Aggressive advertisement would not really help building this positive image. Since at this time it was almost impossible to hide your identity, almost no company used aggressive advertisement methods. Nowadays on the Internet, the identities are not so trustworthy anymore. It has become easier to do aggressive advertising without revealing your identity and consequently without bringing down your image.

4.5. Spammer's Profile

That a Spammer is not a world improver may be clear, but who he really is remains some kind of a mystery. It is at least clear that the Spammer's intention is to spread a message; his own one, or someone else's. Since most Spammers are acting on the border of legality they are not easy to catch. However, an anti Spam solution provider successfully attracted

three E-mail Spammers for an interview [11], which gives an insight into how these people end up into this world and how they work. The quotes in *Table 8* originate from this interview.

"…they work in a secretive environment, constantly straddling the fence between legal and illegal, moral and immoral"
"I fell into it, because it was so cheap to start up, and I had plenty of time to spend with my kids."
"I calculated that I earned around $1200 per week last year"
"You work in groups because it is a necessity, but when it comes down to it, it is every one for themselves."
"I have several great techniques that I am not going to tell you, but I can say that I can get by any spam filter."
"Illegal – no. A pain in the … - yes"
"We're not horrible people; we are earning a livelihood like everyone else. I wish people could appreciate just how hard it is to properly create an effective marketing message."

Table 8: Quotes from an interview with Spammers [11]

Spam is just the 'tool' to spread a message; however, the question is why people want to spread a message and why they use Spam for that. The Spammer's biggest motivator is, of course, money. *Table 9* contains some of the possible motivations a Spammer could have, for which the Commercial and Fraud motivation have the highest occurrence rate for E-mail Spam. In July 2007, Symantec measured 86% of all E-mail Spam being Commercial and 14% being Fraudulent [22]. The other categories where not observed or the occurrence rates were too small to express them in percentages.

Spammer's motivation	**Objective**
Commercial	Sell products, attract people to premium-rate phone number, manipulate share prices.
Ideological / Philanthropic	Spread thoughts and beliefs (e.g. political or religious).
Fraud	Mislead people for financial or other personal gain (e.g. reveal confidential information).
Data-mining	Build behavioural profiles.
Prank	Do something 'big', vandalism.
Study	Learning through experiments.

Table 9: Spammer's motivation

Today Spam is a business, so Spammers are business people and Spamming has a business model. One of the main reasons to start Spamming is the low start-up costs [11] and the high profit a Spammer could generate [9]. To start his business a Spammer needs to make some investments:

- **Spam Strategy** – How to make attractive Spam and stay invisible?
- **Target List** – List with User ID's.
- **Spam Machine** – Hardware and software for making Spam.
- **Internet Access** – Connection to the Internet via an appropriate Internet Service Provider (ISP).

In the context of Spam, there are three types of ISP's: black hat, grey hat, and white hat. A black hat ISP is not active in the field of Spam counteraction; this ISP takes no actions against Spam, if he is not enforced to do it. A grey hat ISP is very tolerant and takes action selectively, or in a very late phase. A white hat ISP is very active against Spam. A Spammer is of course more interested in using internet access of an ISP which is very tolerant to Spam (i.e. dark hat ISP)

Since there is a lot of competition for a Spammer and Spam filters are getting better every day, the Spammer's job is to work hard and be creative. Although the majority of Spammers are interested in earning money, there is also a group which act from ideological or philanthropic motivations and are purely interested in spreading thoughts and beliefs. The Spammers who Spam with a research purpose or just want to make prank, are mainly interested in the effect of the action.

Once a Spammer has done his investments, he could earn money by:

- Selling products by Spam (e-marketing).
- Selling his target list to colleagues.
- Joining affiliate programs (see definition bellow), which in fact is the most common type.

> "**Affiliate Marketing** is a popular method of promoting web businesses in which an affiliate is rewarded for every visitor, subscriber, customer, and/or sale provided through her efforts. It is a modern variation of the practice of paying a finder's fee for the introduction of new clients to a business. Compensation may be made based on a certain value for each visit (Pay per click), registrant (Pay per lead), or a commission for each customer or sale (Pay per sale), or any combination." [20]

Figure 5 shows an example of an affiliate program for selling drugs. Here the Spammer (1) is paid by the affiliate program (2) for generating hits on the pharmacy's website (3), which can be reached via the Spammer's redirect page (4). By means of the Spam messages (5), the E-mail recipient (7) is 'invited' to follow the link (8) to this redirect

page and to buy the drugs at the pharmacy site. This model creates a distance between the pharmacy and the Spamming activities and makes it difficult to sue this company for Spamming.

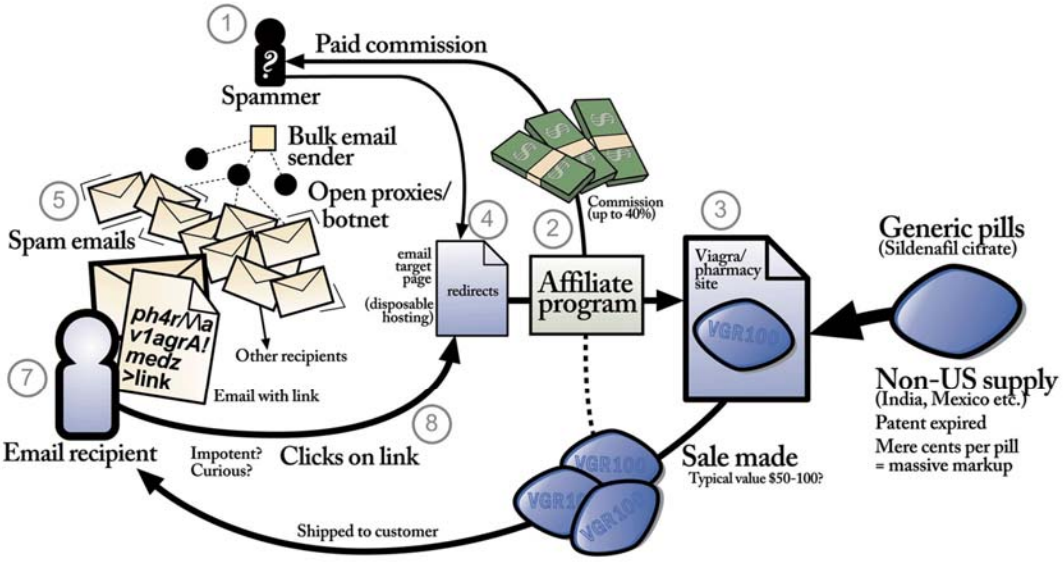

Figure 5: How Viagra Spam works [9]

In a lot of cases it is even more complicated than is depicted in *Figure 5*. Also the Spammer can outsource a part of the job to other parties. A Spam action could be executed in a distributed way by a network of infected devices, a so called Bot network (see *Section 4.6.3*). Bot networks are very often managed by people who sell the use of 'their' infrastructure to, for example, a Spammer. In this situation there are three parties involved in the act of Spamming and this offers the possibility for these parties to specialize. However, from a legal point of view it is more difficult to distinguish who is actually responsible for the Spam attack.

4.6. Spammer's Methods

A part of this research was to investigate the methods which the Spammer can use. In this section we summarize some approaches the Spammer could use in order to efficiently send VoIP Spam and how easy/difficult this approaches are to set up. It's not the aim of this section to give an exhaustive list of all VoIP Spam tools; however, it tries to explain some principles for Spamming. Only assumptions can be made according to the Spammer's Methods, because few real examples are openly reported [32][33].

A Spammer must choose an appropriate Spamming strategy in accordance with his motivation (see *Table 9* in *Section 4.5*). The following list provides some strategies a Spammer could follow:

- **Advertising** – Play audio message for advertisement purposes.
- **Attracting** – Play audio message which makes the callee curious and call back to your premium rate number or go to a website (could be combined with product advertisement, could be unacceptable content, or could be fraudulent content) [33]
- **Impersonating** – Play audio message which sounds like it is from a friend/relative/acquaintance or a certain company in order to win the callee's trust.
- **Behaviour Recording** – Play audio message and records behaviour of callee (how long is the callee listening? how is his reaction?).
- **Call-back Seduction** – Initiate calls which are terminated after the first ring, hoping the person would call back to your premium rate number.
- **Terminating at Callee's Answer** – Initiate calls which are terminated when the callee answers. This way the Spammer could gather information on presence. For instance, for data-mining purposes.
- **Share Price Manipulation** – Play audio message with (possibly fictive) information in order to manipulate stock prices. According to research [79], Spam is an effective way for stock touting.

Besides his strategy, the Spammer is mainly interested in three things: (1) Gather as many User ID's as possible; (2) use an efficient way to send a message to all these ID's; and (3) make it impossible (or at least very difficult) to reveal his true identity. In the following three sections these three actions are explained in more detail.

4.6.1. Gather User ID's

The first step for the Spammer is to build a list of targets, i.e. user ID's. To use the list of user ID's all have to be in the SIP URI format. As stated in *Section 4.3* there is a small difference in storage location for e-mail addresses and SIP URI's. Due to this different, gathering user ID's for VoIP Spam requires a slightly different approach than gathering user ID's for E-mail Spam.

The target list needs to be updated regularly to keep it accurate. If a Spammer wants to increase the quality of his list he has to verify the user ID's on his list. The opt-out ('unsubscribe') method, for instance, could be (mis)used to verify an ID. If a user tries to opt-out his ID, the Spammer knows that this ID is valid.

The target list can be build up by scanning address books, either public ones or private ones using Trojans. Also the ENUM system (see *Section 3.2.4*) is very attractive for ID gathering. Another approach for ID gathering is ID guessing, e.g. simply trying all possibilities in a certain namespace. Guessing of Type I SIP URI's (see *Section 3.2.4*) is very difficult and time-consuming, due to the large namespace, which is comparable to the namespace of E-mail addresses. The advantage of using the Type II SIP URI (see *Section 3.2.4*) for ID guessing, rather than Type I, is two fold:

- The Type II SIP URI has a significant smaller namespace, because here the user-field is bound to digits. For example, the province Zeeland in The Netherlands has an area code of 118 and all fixed telephone numbers in this area have a length of 6 digits. Thus, these phone numbers in international format are of form +31 118 $a_0a_1a_2a_3a_4a_5$, where every a_x (for $0 \leq x < 6$) is a digit. Since the namespace in this example is 10^6, that gives only one million possibilities to try.
- Since there is still a direct relation between a phone number and a geographic area, the number reveals information about the region where the person lives and probably also about the language the person speaks. This enables sending spam in a specific region and language. Since this is hardly possible with E-mail Spam, this could make VoIP Spam more effective. However, there is currently a globalization going on for telephone number, because in VoIP it is less important that the number (or Type II SIP URI) is related to specific geographical area.

See *Section 5.1.13* for information on how to prevent ID guessing.

Personal information is worth money. Therefore (of course) there is a huge trade in personal information. Also user ID information is sold, for example E-mail addresses for E-mail Spam. Spammers could also expand their target list by buying target lists of others. It is also conceivable that a Spammer starts an action “Hand in all your business cards and earn money!” and pays you some amount of money for every unique business card you send in. Although this is illegal according to European privacy laws; it could be an easy way to earn some money.

4.6.2. Spread a Message

To spread a message the Spammer needs to build a Spam system, which is able to perform the Spam action after the Spammer feeds it with his target list and the Spam message. This could be a very easy program which is able to make calls in an automated way.

The Internet is rich in information on how to set up a IP based telephony server in order to generate calls. In this research we build a SPIT Analysis Platform, for which the details are provided in *Appendix B*. This platform uses the open source PBX server Asterisk [21] for generating VoIP Spam. With some knowledge about Asterisk and about Linux it is possible to set up the platform within one week. On our platform we used the program SpamScheduler (see *Appendix B*), which has been designed specially for this research, to feed Asterisk.

This report focuses on telephony by means of SIP. However, we want to spend a few words on Spamming via Skype here. There is a special Skype API [66] available with which it is possible to execute Skype action (e.g. dialling, sending message, etc.) in an automated way. This could be the basis of a Skype Spam machine. The availability of a search functions for Skype users and the ability to phone people without having them in your buddy list, provides Spamming possibilities [23]. Skype Prime, which is a Skype service for opening a premium rate number which is charged per minute, could help the Spammer to earn money.

Since now the Spammer is equipped with a list of targets and a Spam system, he could start spreading his message. The Spammer knows what he wants to obtain so he has to make a perfect message, which triggers people to act according to the Spammer's intention. The best method for a Spammer is: making people either curious or afraid or play with other feelings. *Table 10* shows some ideas of content Spammer's could use for the different motivations which are stated in *Table 9*.

Spammer's motivation	Spam Content Examples
Commercial	Product advertisement or (links to) sexual oriented content.
Ideological / Philanthropic	Political or religious thoughts and believes, trying to convince people, or the other way around: Spread thoughts of the enemy/competitor in a bad or annoying way.
Fraud	Impersonate a company which the callee has a customer relation with, in order to reveal personal information, a call-back mechanism, or a message for influencing the stock quote price (stock quotes Spam).
Data-mining	Surveys.
Prank	Unacceptable content (e.g. illegal content or offensive language from strangers).
Study	Can be everything.

Table 10: Spam content

Message creation is (at least for E-mail Spam) the most time consuming work. The message a Spammer wants to obtain should be attractive and optimized for bypassing Spam filters. A Spammer should study the new trends in the field of Spam filtering to test his message against new filtering techniques. Since Spammers are constantly trying to circumvent the implemented Spam filters and getting attention of the recipient, the content of Spam messages evolves very fast. For E-mail Spam there were first the pictures which were causing trouble for filters, and as soon as developers implemented intelligent method to filter this kind of Spam, the next challenge was Spam with Portable Document Format (PDF) document and Rich Text Format (RTF) document attachments. By the time of writing MP3 Spam is en upcoming method for E-mail Spam, see [83]. This is the first step in the direction of VoIP Spam.

Once the message is ready the whole action has to be planned. Timing is important to reach the targets at the right moment. E.g. the moment when they are most probably reachable, the moment when they are most probably in a good mood to receive the message, etc.. The following timing strategies are just examples:

- For product advertisements the Spammer could pick the time of the year when the recipient is most probably in a good mood for the product. For instance, Diet products after Christmas.
- Send Spam in the weekend in order to decrease the probability that the action is observed by the system administrator.
- Send Spam around diner time in order to ensure that people are at home. This strategy is only applicable to fixed devices.

The distribution of the Spam messages over time and space could also be important in order to bypass Spam filters or avoid legal judgement. The challenge for the Spammer is to send his message in such a way that it looks like legitimate behaviour, in order to hide his action and to circumvent the possible anti Spam mechanisms. A Spammer could, for example, hide his action by making the action random (e.g. random spacing between calls, random call duration, etc.). Furthermore, a Spammer could misuse the models for generating 'legitimate' traffic, which anti Spam providers use in order to test their anti Spam mechanism.

In this research we generated Spam by only one machine, but in practice this could very likely be different. One way of Spamming is to use a network of Bots (infected devices that are under control of one person), a so called Bot network. Seeing that most E-mail Spam is sent by Botnets [34] it is very likely that also a big portion of VoIP Spam is going to be sent via Bot networks. The next section will provide more information on Bot networks.

Once everything is ready to send Spam, the remaining thing is 'Fire and Forget'.

4.6.3. Hide True Identity

The main reason why a Spammer wants to hide his identity is to make it impossible (or at least very difficult) to make him responsible for his action and apply legal penalties. Spammers who are interested in earning money must make sure that the money (i.e. their profit) can flow to them while their identity is hidden. There are some different ways a Spammer could hide his identity:

- Distribution in time.
- Distribution in space.
- Onion Routing.
- Anonymous SIP Proxies.

Distribution in Time

The easiest way to stay invisible is to add some (random) time between the calls. Doing so, the call pattern looks very much like legitimate behaviour and Spam could only be detected by content analysis or user feedback, which are non-detective countermeasures (Section 5.1). Another effect of distributing the Spam action in time is that it is more

difficult to see it as just one action and not as multiple actions (legal issue). However, the negative aspect of distribution in time is that the call volume is limited.

Distribution in Space

Next to the distribution in time, distribution in space could also help to hide the Spammer's true identity. In order to distribute a Spam action in space, the Spam is sent from different hosts. As a result, there are several small attacks, which are less likely to be noticed. Distribution in space enables a much higher call volume.

Bot networks could provide a way to send Spam from different hosts. Bots, which are also called Zombies, are computer programs which run remotely on different hosts. The different Bots are under the control of one entity (i.e. a person or a machine) and could perform one or more tasks (e.g. sending Spam). Often the Bot software is incorporated into a virus and spread over the Internet in order to infect devices and install this Bot. Bot networks (also called Botnets or Zombie networks) could grow into a large collection of Bots. The largest Bot networks known have a size of millions of Bots [38].

By using a Bot network, normal (legitimate) devices are misused to generate Spam, consequently every device is responsible for a small portion of the action. Bot networks are the most used technique for E-mail Spamming and have the potential to become the main technique for VoIP Spamming.

Bot networks form a great threat on the Internet. Bot networks are not only used for sending Spam, but also for other attacks (e.g. DoS attacks, steal personal information). There are a number of initiatives in order to counteract these Bot networks. In June 2007 the FBI started an initiative called 'OPERATION BOT ROAST' [36] in order to identify Bot networks and inform the host owners of the Bots. The Honeynet Project, which is a non-profit initiative which tries to 'know the enemy' via research, published some Bot source code for researching purposes [35]. Another group published a full working Bot program together with source code for academic research [37]. These initiatives could help in the counteraction of Bot networks.

Onion Routing

Onion Routing is a cryptographic way to obtain anonymity by routing the traffic in a random (and thereby obscure) way. The routers (i.e. computers with Onion Routing software installed) in the Onion network are capable of retransmitting Routing Onions, which are data structures following an unpredictable path from their origin to their destination. Before sending data, the origin first selects multiple (onion) routers at random and encrypts the data multiple times (for every intermediate router one encryption). This encryption is done in such a way that every intermediate router could do a decryption which reveals only the address of the next hop and the destination could do a decryption which reveals the original data.

The originator selects n-2 intermediate router. The data starts at the originators host (R0) then travels through multiple Onion Routers (R1,…,Rn-1) and then arrives at its

destination host (Rn). The public key of every host Rx is know to be pk(Rx) (for $0 \leq x \leq n$). We assume that data encrypted with pk(Rx) only can be decrypted by host Rx.

The original data is first encrypted with pk(Rn). For every intermediate host Rx (for $0 < x < n$, in decreasing order) the packet and the address of the subsequent host (i.e. Rx+1) are encrypted with pk(Rx). Thus the final packet looks like this:

$$((\ldots((\text{data})_{pk(Rn)}, Rn)_{pk(Rn-1)}\ldots, R3)_{pk(R2)}, R2)_{pk(R1)}$$

Thus, when this packet is send from the originator (i.e. R0) to the first intermediate router (i.e. R1), it is decrypted by this host (the first Onion Layer is peeled) and the host is able to read the address of the next intermediate router (i.e. R2) and send the packet to this host. This way, every host only knows the next host and only the destination host knows the data.

The Onion Router (TOR) is an open source implementation of onion routing software. According to the TOR website (tor.eff.org) the current TOR network has grown to hundreds thousands of users and is capable of routing all kinds of IP traffic (e.g. VoIP traffic).

Anonymous SIP Proxies

Finally there are anonymity proxies, which are in case open public proxies. These proxies redirect Internet traffic without revealing its origin. Although, at the time of writing it is still hard to find any open SIP proxies, this could change in the future.

4.7. The impact of VoIP Spam

Although people have experience with annoying telemarketers and surveys, very few people have experience with automated machine calls [Q 1.7]. Since currently the existing VoIP networks are islands, the occurrence rate of VoIP Spam is still low and thereby also the impact is low. However, VoIP Spam is expected to have a much higher occurrence rate as soon as the different VoIP communities are interconnected and form a worldwide telephony network, in which a call from Switzerland to Japan has the same price as a call from Bern (CH) to Geneva (CH). In [Q 1.8] a convincing 85% of the respondents think that VoIP Spam will be a problem in the future, against 10% who do not see VoIP Spam as a threat and 5% who could not answer the question.

Spam is by definition unsolicited and thereby very likely to be unwanted or even annoying. Spam causes costs for both the recipient and the network owner. These costs will increase as the volume of Spam increases. In this section both the costs for the end-user (i.e. recipient) and the costs for the network owner (in case of VoIP Spam this is the service provider) are described. It is estimated that E-mail Spam causes Internet subscribers a total connection costs of 10 billion euros a year worldwide [40].

4.7.1. Costs for the End-User

The Spam problem exists in cases that the costs for the receiving side are higher than the costs for the originating side (see *Section 4.4*). The main costs for the end-user (i.e. receiving side) are costs in time and in deterioration of mood.

We can say Spam is theft; a spammer steals valuable time from the recipient, who has to read/scan the messages or answer calls. VoIP Spam causes costs in time because the recipient's telephone is ringing and asking for attention. If the recipient picks up the phone he needs a couple of seconds to recognize the phone calls as Spam. And even if the recipient recognized the call being Spam, he might get curious and listen longer. Especially in the early days of the VoIP Spam problem, people might listen somewhat longer, because people are not used to the phenomenon and more likely to be curious. From the perspective of one single user these costs might be still acceptable, but in an enterprise these costs are multiplied by the number of employees and will cause financial costs.

When the VoIP Spam ends up in the voicemail box the impact is somewhat different. Now the message is not pushed by the network, but pulled from the network, consequently the message is less intrusive, but still there is a time costs for filtering out the Spam voice mails.

Each individual likes to be treated as a unique person. With Spam individuals are treated as a database entry, because the unicast medium is used for broad dissemination of information (*Section 4.1*). Therefore, it is very likely to be annoying when Spam is received in large volumes. This annoying communication has a direct impact on the end-user's mood. Because there is no relation between the Spammer and the recipient the Spam could interrupt the end-user at an inconvenient moment, and thereby have a direct impact on someone's privacy.

Next to these costs in mood and time there could be other costs in case the recipients react according to the Spammer's interest. For commercial product advertisements this could imply buying a potentially harmful product. There are confirmed cases where people died because of the consumption of cheap health products. Fraudulent Spam could cause direct financial costs, when the recipient reacts to it. Furthermore, Spam with pornographic or other possibly offending content could be harmful for young people.

4.7.2. Costs for the Service Provider

Apart from the fact that VoIP Spam is annoying and time consuming for the end-user there is also impact on the availability and integrity of the telephony network. In order to process all VoIP Spam, telephony systems have to be able to handle more traffic than strictly needed. This increase in the load requires more bandwidth and more computational power. As a result there are costs for the telephony service provider due to Spam. The costs for the ISP's are negligible, because only a small portion of total Internet traffic is for VoIP. For the telephony service provider, however, the impact is

higher, because his main traffic is VoIP traffic and the service provider has some 'telephony intelligence' build into his network.

When VoIP Spam ends up in a voicemail box, the impact is slightly different. In this situation there is a huge impact on the storage demand in the network. However, in this case post-processing filters may apply, as with E-mail Spam.

Due to the decrease in the availability of the recipient and the annoyance level for the recipients, the recipient's trust in the system will decline. This is seen as the most urgent effect of Spam, from a service provider's point of view. Since VoIP is still an upcoming technology, the lack of trust in the system could cause a decrease in the wide adoption of this technology.

In order to summarize this section, VoIP Spam has the following costs (the figures are based on our own assumption):

- **Mood** (end-user).
- **Time** (end-user) – ~5s per message.
- **Bandwidth** (provider) – 64 kb/s per call, when the codec G711 is used.
- **Computational Power** (provider).
- **Storage** (provider) – 64 Kb/s * ~60s / 8 bits = ~480 KB per voicemail message.
- **Network Integrity** (provider).

4.8. Ethical Issues

Imagine a road through a forest for which there exists a shortcut, for cyclists. Using this shortcut brings some negligible changes to the environment. Driving by bike through this shortcut seems to be ethically right. However, if one asks himself the question 'what if everyone uses this shortcut?' this becomes different. One or two people, using this shortcut will cause no real problems, but thousand people using it would cause a damaged living environment for the forest species. Thus there are actions which do not cause problems in an isolated form, but cause big problems when this action is committed en masse. Spam is such a typical action for which the what-if-everyone-does-it question is relevant. Most Spammers consider their activities to be harmless [24], but probably they forgot to ask themselves the what-if-everyone-does-it question. Spamming is generally seen as unethical, though a single Spam action is not wrong in an isolated case.

Spammers are often acting on the border of what is moral/immoral, because it is not always obvious where the border is between spam and legitimate behaviour. Besides doing aggressive advertisement via Spam, also 'less bad' things could be done via Spam. An example of such an action is sending automated messages via VoIP for emergency purposes. In [Q 1.2] 58% of the respondents think an emergency broadcast is Spam and they point out TV and newspapers as a better medium for this communication. It is also

the question whether it is done by a private person or by a governmental entity, like the police. 53% of the respondents would seriously think of using VoIP Spam (assuming they know how to do it) in case their child got lost [Q 1.3].

Spamming is a concept with a very short history. It is introduced to the world along with the increasing use (and misuse) of the worldwide IP network, i.e. the Internet. The predecessors of Spam, i.e. direct mail and door-to-door salesmen, were not a big problem because the (physical) resources for these advertisement techniques were somehow limited.

Spam is forbidden by law (see *Section 4.9*), but still there is a company's need to do advertisement and to reach his target group optimally. The question is how to do advertisements without Spamming. This question is, however, very easy to answer:

- **Dedicated Advertisement Channels** – Use dedicated communication channels for advertisement, e.g. billboards. It is preferable that the advertisement message is pulled from this network or pushed by the network with a very low level of intrusion.
- **Go for Quality** – Go for quality rather than quantity. It is preferable to select the target group carefully and reach only these people who are potential interested in your product.

The procedure to make legitimate E-mail marketing is explained in [45].

4.9. Legal Issues

It is far too easy to say that Spamming is wrong and that a Spammer is a criminal. Going to a crowded place and screaming very loud how people can buy Viagra of Company X is strange but not forbidden. People might think you are a lunatic, but maybe it is an effective method to sell a couple of pills. Although there is basically nothing wrong with spreading your message, it is not very kind to spread a message for which the quantity is more important than the quality and this is very often seen as aggressive advertisement, which in fact is forbidden by law.

When talking about Spam the law becomes very important, because it limits both possibilities for making Spam and possibilities for counteracting it. In this section we try to explain some basic legal issues. Since this report is written from a technological perspective it is not the aim to give a full overview of what is legal and what not and in which country. Swiss and Dutch laws have been used as basis for this section.

4.9.1. Spam Generation

Worldwide a lot of countries have implemented anti Spam legislation, but the way these laws address Spam is very inconsistent. In some laws Spam is forbidden independent of the technology used and in other countries only E-mail Spam is forbidden (e.g. Australia). In some laws the term Spam is not even explicitly mentioned.

This report focuses on the Spam prevention laws in Switzerland and The Netherlands. These are defined as follows:

- In article 3 literal o of UWG [67], the Swiss Law forbids to send bulk messages when one of the following conditions is true:
    1. The user did not requested the messages.
    2. There is not a correct originator ID attached to the message.
    3. There is no easy and free way to opt-out.
- Article 11.7 of the Dutch Telecommunication Law [12], which is based on European law (Article 40 of the Directive on Privacy and Electronic Communication 2002/58/EC [69]), forbids automated machine calls without human interference, faxes and electronic messages in order to initiate unsolicited communication for commercial, ideological, or philanthropic purposes.

Obviously in both Switzerland and The Netherlands Spam is forbidden by law, independent of the technology used. Both laws are based on an opt-in model, which says that bulk communication is allowed only in case a user requested it. Other countries, for instance the United States, implemented a law which is based on an opt-out model, which says that Spam is allowed, unless a user has objected receiving it [47].

In some countries special black lists exist for direct telemarketers. People can subscribe to these lists if they do not want to receive phone calls from telemarketers. The Robinsonliste (used in Germany, Switzerland and Austria) and the 'Do Not Call'-list (used in the USA) are two examples of such lists (see *Section 5.1.2*).

For both the Swiss law and the Dutch law, using a machine to make phone calls is an indicator of the call being Spam. Thus, a machine initiating bulk calls is in most cases illegal. A Spammer, however, might get round the law by deploying a call centre with (possibly poorly paid) call agents, which are initiating the phone calls. As soon as the phone call is initiated it is handled over to a machine which plays a Spam message.

4.9.2. Spam Counteraction

It is important to consider the country specific laws (e.g. privacy laws) before implementing anti VoIP Spam mechanisms. For a telecom provider it's like balancing on a tight rope; they cannot take preventive action too early (user's freedom is limited) and not too late (user is annoyed by Spam). However, in our opinion there are methods to counteract Spam without limiting the user's freedom. *Chapter 7* contains a design of an anti Spam solution, aiming to give the user more freedom instead of limiting it.

According to the Dutch law (Article 11.2 of the Dutch Telecommunication Law [12]) a telecom provider is obliged to use technical and organizational methods to protect the user's personal environment. The Swiss law (Article 83 literal 1 of the FDV [68]) directs

Telecom Service providers to protect their customers from unfair bulk advertisements, as far as technology is available.

For E-mail Spam counteraction content analysis is both an important filtering technique and required as proof for Spamming behaviour, but for VoIP Spam counteraction we have to find other techniques. Due to privacy laws it is very difficult (or even forbidden) to do content analysis. For recording content the consent of both the caller and the callee is required. However, both BAKOM and OPTA do not find it objectionable to do content analysis for the sake of VoIP Spam protection [Q 2.2/29][Q 2.2/38], if the user is informed about it and if the user's privacy is respected.

There are people who argue that anti Spam techniques will limit the freedom of expression, which is a right guaranteed under international law. This is a wrong statement, because Spam prevention only limits communication via a certain channel (which is vulnerable to Spam). It remains possible to express the message via another channel.

Off course, laws can counteract VoIP Spam. However, as long as money is the motivator there are people willing to take the risk. *Section 5.2* provides more information on how to counteract VoIP Spam by means of legislation.

Chapter 5
Theoretical Countermeasures

***Illustration**: Jack has been making VoIP Spam for two month now. Every week he increases the size of his action and his success rate turns out to be better than with E-mail Spam.*

During his work Jack reads about anti VoIP Spam mechanisms and during the evening he enhances his Spam machine in order to customize the actions for bypassing the countermeasures. Jack also starts to implement his Spam software into his virus in order to send Spam via his Bot network.

To be continued…

It seems to be impossible to ban out all VoIP Spam, but it is definitely possible to increase the Spammer's investment (i.e. time and money) and reduce the impact of Spam. This can be done by implementing countermeasures in order to make a Spammer's life more difficult and make Spam less effective. This chapter lists the most important countermeasures for VoIP Spam prevention. Although some of these countermeasures are not realistic, they are still in this list, because they may be a starting point for further research. Sometimes a single countermeasure is undesirable, but the countermeasure could be combined with another one to get a better result. None of these countermeasures embraces 'the perfect solution'. In our opinion the key for VoIP Spam counteraction is a suitable combination of multiple countermeasures. *Section 5.9* contains some examples of combinations.

The countermeasures in this chapter can be classified into preventive, defensive or detective. Preventive countermeasures are intended to decrease the amount of Spam that is sent by the Spammer (e.g. law). Defensive countermeasures are intended to decrease the amount of Spam that reaches the recipient. Detective countermeasures are intended to recognize Spam in order to provide input for other countermeasures. *Figure 6* shows in which phase of the call which countermeasures are working. In *Section 5.5* these classes are mapped on the countermeasures.

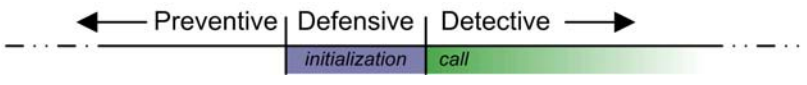

Figure 6: Countermeasure classification

In this chapter we divide the countermeasures into four groups, i.e. Technical Countermeasures, Legal Countermeasures, Social Countermeasures and Commercial Countermeasures. This section embraces countermeasures in all of these groups. For every countermeasure our own opinion is reflected by means of an evaluation section. Furthermore the countermeasures are mapped to the inherent problems, for which the important ones are explained in Section 5.6. In the end of this chapter there are sections on: acting on Spam detection, Spam prevention and network architecture, and countermeasure combinations.

5.1. Technical Countermeasures

Most of the countermeasures, presented in this section, are technology oriented. These countermeasures should be implemented by a telecom provider. The technical countermeasures are not capable of detecting Spam with a 100% certainty, but they all can result in the per cent likeliness of the behaviour being Spam. If multiple countermeasures are implemented the total likeliness will be the mean of the (possibly weighted) percentages from the different countermeasures. Thresholds can be defined in order to make decisions about the actions to take (*Section 5.7*)

[Q 1.9] shows that most of the people think that technical Countermeasures are (reasonably) effective. It is always a trade off between effectiveness and flexibility of use [Q 1.9/13]. In our opinion the usability of the telephone system must be, at least equal to the usability in the traditional telephone system.

For the acceptance of a countermeasure user involvement is essential. The user should be able to turn on/off and configure the countermeasures. As a result, the users will have freedom on his telephony service. This could also simplify legal issues (*Section 4.9*). Another must is to have an easy and straightforward function for user feedback (*Section 5.1.5*). This way valuable information about Spam attacks can be gathered and a user is able to express his annoyance.

5.1.1. White listing

A white list is a list of user ID's which are marked to be 'good guys'. Normally the initiator who's user ID is on the white list of the recipient gets a special treatment. In most implementations this boils down to bypassing further anti Spam mechanisms. A white list can either be a private list (i.e. buddy list) or a group list. Group lists are used by multiple users and therefore are stored centrally and are accessible for all authorized users. Private lists, which are personal (every user has a list), are likely to be smaller and could be stored either in the network or on user equipment.

It is possible to extend the white list implementation with the notion of user groups in order to configure the white list system in a more intuitive way. We can identify three groups, as defined in [18]:

- **Closed Group** – Only members of the same group are able to initiate communication to each other. This is implemented by a strict white list, only when a caller is on a white list of a user he is able to initiate communication with that user. The closed group concept could, for example, be used for children who may only receive phone calls from 'trusted' persons (e.g. their parents, some friends) and not from strangers.
- **Semi-Open Group** – This is a mix of an Open and Closed Group. The limits someone has are dependent on the role of this person and his personal preferences. The semi-open group concept could, for example, be used in an enterprise environment where customer oriented workers can receive phone calls from customers and system administrators could only receive internal phone calls.
- **Open Group** – There are no limitations for receiving phone calls. The open group concept could, for example, be used for a helpdesk which should be accessible for everyone.

Evaluation

Many Instant Messaging (IM) systems and free public VoIP system, like MSN Messenger and Skype, are working with white lists. In these applications the white list provides a second functionality, namely an address book to enable quick dialling. These white lists are private white lists, which have, at least in an enterprise environment, a reasonable storage requirement. Group lists have a slightly different storage demand than private lists.

The cooperation of the user is very important in order to keep the white list accurate. Therefore the user should be rewarded for maintaining his private list, e.g. by quick dialling. Furthermore features to import and export lists and to share (parts of) the list with other users are assumed to be very helpful. In order to enable these usability increasing features, the private white list should be stored in the network rather than on the user equipment. For group based white lists user cooperation is less important, because here the white list is managed by the network administrator.

Next to the storage requirements and the cooperation of the end-user, effective white list implementations require a strong identity. A white list implementation without a strong identity is vulnerable to identity misuse (see *Section 5.6.1*).

Another problem with white list implementation is the introduction problem (i.e. how a callee's ID is added to the white list). The white list has to be filled and there should be an easy mechanism to add list entries. *Section 5.6.2* contains more information on the introduction problem and possible solutions.

A private white list by itself has a high False Reject Rate (FRR), because it is very unlikely that all legitimate callers are on a private list. Furthermore, a private white list has a low False Accept Rate (FAR), because the callers on the white list are trusted by the user and thus likely to be legitimate. A group white list has a medium high FRR and

FAR, due to the fact that the list is bigger (i.e. more chance a caller is in the list) and also less reliable, because the list is less personal.

In our opinion a white list should be implemented as a private list or a small scale group list, in order to prevent from False Positives. A combination between a private list and small scale group list would be helpful to optimize the effectiveness. It should be possible to maintain the list very easily. In order to avoid a complex implementation all lists should be stored in the network. By storing the lists in the network, synchronization between different devices is not required.

5.1.2. Black Listing

A black list is a list of user ID's which are marked to be 'bad guys'. Normally the initiator who's user ID is on the black list of the recipient gets a special treatment. In most implementations this boils down to either blocking or applying a stronger anti Spam mechanism. Private lists, which are personal (every user has a list), are likely to be smaller than group lists and could be stored either in the network or on user equipment. Although a black list can be either a private list or a group list, the most implementations are group lists.

Another application of the black list principle is a black list for the e-marketers themselves. The USA's 'Do Not Call'-list (www.donotcall.gov) is an example of such a list. Telemarketers are obliged to search this list every month and to drop phone numbers from their call list which are registered to this 'Do Not Call' registry. There are also other initiatives for public black lists for e-marketers. E.g. the Robinsonliste (www.robinsonliste.com).

Evaluation

Although black listing is a respected way to counteract Spam, it has some important disadvantages. It is not always possible to attach a 'bad guy'-label to a user who initiates Spam, because the user could be infected by a virus. Placing him on a black list would be too definite in this case.

Maintenance of the black list is very important in order to identify Spam sources. To maintain the list, either user cooperation (in case of a private list) or a reliable Spam detection mechanism (in case of a group list) is required. Inappropriate maintenance of a black list could lead to False Positives and False Negatives.

A black list requires storage, especially when it is easy to become fresh identity. Like a white list the group based black lists has a slightly different storage demand than private based black lists. If the private black list is chosen to be used, it should be implemented to store the lists in the network in order to avoid requirements for synchronization between different devices.

A black list by itself has a high FAR, because it is very unlikely that all Spam sources are on the list. Furthermore, a private black list has a low FRR, because the callers on the

black list are entered by the user and thus unlikely to be legitimate. A group black list has a medium high FRR, due to the fact that the list is bigger and not personal and thus the reliability is limited.

A black list implementation requires a strong identity; if it is easy to obtain a new/fresh identity, a Spammer could send Spam with a lot of different ID's and every time an ID is on the black list he could get a new one. A strong identity reduces the storage demand.

5.1.3. Grey Listing

With grey listing every (known) caller gets a behaviour value based on its behaviour in the past. This value is increasing in case of 'bad behaviour' (i.e. Spamming behaviour) and decreasing in case of 'good behaviour' (i.e. no Spamming behaviour). All grey list implementations are group lists, because the behaviour could only be measured at the networks side and not at client side.

Progressive Multi Grey-levelling (PMG) [70] is a special variant of grey listing. As a result of the observed call pattern, the caller gets a short term behaviour value, which is increasing/decreasing quickly, and a long term behaviour value, which is increasing/decreasing slower. The mean of these two behaviour values gives the total behaviour value.

Evaluation

Like all listing approaches also for grey listing there is a strong identity requirement, which makes the approach vulnerable to identity misuse. Like group based black listing, grey listing requires also a reliable Spam detection mechanism in order to adapt the behaviour value.

Grey listing requires storage for the user ID's and for their behaviour values. Implementations could also require additional storage for keeping behaviour history.

The big advantage of grey listing compared to white listing and black listing is that the labelling principle ('good guys' vs. 'bad guys') is not black-white, i.e. there is a possibility to express an uncertainty. Another advantage is that the label is not static. There is a possibility to obtain a lower behaviour value by improving one's life or cleaning the device from virus infection.

5.1.4. Turing Test

A Turing test is a test for being human, in order to filter out machines initiating communication. Whenever new communication is initiated the originator (both a human or a machines) has to prove being a human by performing a test which is simple for a human, but impossible (or at least computational intensive) for a machine. A well-known form of a Turing test is the Completely Automated Public Turing test to tell Computer and Humans Apart (CAPTCHA), which is used on registration forms on some websites (see *Figure 7* for an example).

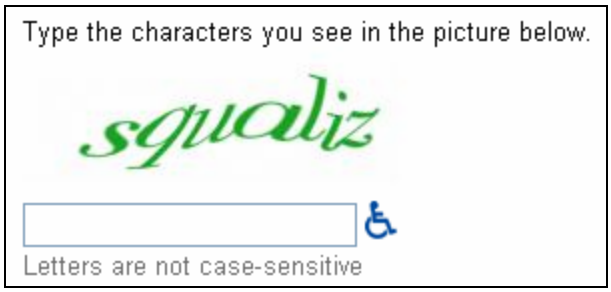

Figure 7: CAPTCHA example (source: www.google.com)

In a Turing test implementation to counteract VoIP Spam, a message is played to the caller when he tries to initiate a phone call. Depending on the caller's ability to act according to this message his phone call is initiated or not. The test should require some artificial intelligence, which is difficult for a machine to have. A Turing test could be implemented in various ways:

- **Voice Interpretation Challenge** – A message is played which tells the caller what he should do in order to initiate the phone call. Only the caller who is able to interpret this message and successfully complete these instructions passes the test. For example, the caller is asked to input a random combination of digits.
- **Simple Puzzle** – A message is played which explains the caller a puzzle. Only if the caller can solve this puzzle and he is able to communicate the answer he passes the test. This puzzle could for example be an arithmetic problem. Of course, for this method too voice interpretation is important.
- **Communication Pattern Observation** – A message is played which asks the caller to say something. The call is initiated only if the caller's communication behaviour is like a human. More information about the communication pattern observation approach for a Turing test is provided in [43].
- **Personal Introduction** – A message is played which asks the caller to introduce himself. This introduction is then recorded and played to the recipient. According to this message the recipient could decide to take the call or not. The negative side of this approach is that it is callee intrusive.
- **Digital Receptionist** – The caller ends up in an IVR system, in which the caller has to dial numbers or use his voice in order to navigate through the menus. In order to initiate the call to a callee the caller has to choose the right path through the menu structure. Although it is difficult for a Spam machine to adopt his behaviour to IVR systems, it is possible for the Spammer to program his machine to handle a certain menu.

A technical implementation of a Turing test for a SIP based VoIP network is defined in [41].

Evaluation

For an implementation of a Turing test it is important to consider the difficulty of this test. This is a balance between a very easy test, which is less annoying for the legitimate user and easier to bypass for a machine, and a very difficult test, which is more annoying for the legitimate user and more difficult to bypass for a machine. The capabilities of disabled people and children should also be taken into account.

It is possible for a Spammer to circumvent the Turing test by human intervention during the Turing test phase. A Spammer could use a number of, possibly cheap paid, workers to pass the Turing tests. In this case the call agents perform the Turing test for every call and hand it over to a machine which plays the Spam message to the recipient.

Although a Turing Test seems to be a very efficient method to filter out machine initiated communication, it is an annoying addition to a telephony system and it could be a problem for (legitimate) disabled people and children. In our opinion the Turing test should be used only as a backup countermeasure, which is activated in case other countermeasures do not give decisive answer on the call being Spam or not.

In a company it might be favourable to implement a digital receptionist (i.e. IVR system) for every (non-customer) call. Next to the Turing test functionality of this approach, it could also help the callers with finding the right callee. IP based telephony makes it easier and cheaper for every company to implement such an IVR system.

5.1.5. Callee Feedback

To identify a call being Spam with a high certainty, two conditions are important: (1) The call is unsolicited; (2) The call is sent in bulk. Only the network itself is capable of identifying the latter condition (e.g. by behaviour analysis, which is explained in *Section 5.1.9*). The recipient is the only one who could judge about the call being unsolicited or not. The information about the call being unsolicited or not is gathered by a callee feedback system. By the Swiss law (Article 83 of FDV [68]) it is obligatory for a service provider to implement a possibility for their customers to give feedback.

During the communication or direct after the communication, the recipient gives his feedback to the system about the communication being unsolicited or not. The feedback information could be input for other countermeasures (e.g. grey list). The possibility for feedback can be implemented in various ways, for instance, a special ‘Report Spam’-button on the phone which can be pressed in order to identify the call being unsolicited. Malicious Call Identification (MCID), specified in [72], was a callee feedback function of ISDN, with which the caller could simply enter a key-combination during the conversation in order to identify the call being malicious [42].

Evaluation

Callee feedback is very important to detect Spam, because the Callee is the one who can identify unsolicited calls very easily and exactly [26]. However, it is the question how many people take the effort to provide the system with feedback. Since the feedback

function depends highly on the cooperation of the end-user, it should be implemented in such a way that it requires very limited effort for the user. In order to implement an easy way to give feedback, it is very important to standardize callee feedback methods. A start is made in the process of standardizing callee feedback approaches [27].

A callee feedback function requires trust in the end-user. Although the end-user is the only one who can identify unsolicited calls with a very high probability, he could make a mistake or act in a malicious way to denounce the caller.

Identity (i.e. Identity of the Spam source) misuse could decrease the value of the feedback information. A strong identity is required, in order to ensure the value of the feedback information. By giving direct feedback the callee has to reveal some personal information, for which he might want to keep it secret from others. Therefore privacy is also an issue for the callee feedback approach.

There is a requirement for storage, which depends on the size of the feedback history. It is not favourable to store the feedback information with a long history, because the caller's behaviour in the past gives limited information on future behaviour. The length of the history should be chosen in accordance to the role of the information in the complete anti Spam model.

5.1.6. Content Analysis

During the communication the content of a phone call is analysed in order to check it for Spam content. In VoIP, content analysis to counteract Spam could be performed by a couple of strategies:

- **Speech-to-Text** – The VoIP Spam message is translated into text. This enables the content analysis techniques which are used by anti E-mail Spam methods (e.g. Bayesian Filtering [43]). Although there is a lot of research going on in the field of Speech recognition, it is still difficult for a computer to translate speech to text.
- **Identification by Voice** – For every VoIP Spam message the voice characteristics are stored in a black list. Comparing the voice of every caller with the voices in the black list would say something about the likeliness of the call being Spam [43][71].
- **Communication Pattern Observation** – The communication pattern of the caller is analysed in order to check whether it is produced by a human or not. Machines are assumed to be incapable of adapting their communication pattern to the other party. In most cases a Spam machine will plays the Spam message regardless the reaction of the recipient. More information on communication pattern observation can be found in [44].

In case the call ends up in a voicemail box there is no need for analysing the communication at real-time; post processing is possible.

Evaluation

Since content analysis is only allowed under country specific constraints (e.g. all parties have agreed or they know that the conversation is recorded), it is difficult to apply content analysis at large extent.

A text, typed by one person, will always be the same as the same text typed by somebody else. In contrast, voices are unique for every person and dialects make the differences even bigger. Since speech has much more variety than text, it needs much more computational power to analyse speech. The need for high computational power is another disadvantage of content analysis.

In an E-mail system content analysis is applicable just before the message is delivered and it is the most promising method for counteracting E-mail Spam [50]. However, for VoIP this is different. At the moment that there is content available for analysis the telephone conversation is already initiated and the result of this content analysis can not be used for this call. However, if the call is forwarded to a voicemail box, post processing is possible.

Call pattern observation seems to be a promising approach of the three content analysis approaches. It requires less computational power than the other two, because it is easier to identify a communication pattern than to identify words or voices. Furthermore call patter observation requires less storage. The main disadvantage of call pattern observation is that it is a detective countermeasure. The result of the analysis cannot be used to directly counteract VoIP Spam, but only as feedback for the anti VoIP Spam system.

5.1.7. IP/Domain Correlation

By observing the caller's ID, domain (in DNS sense) and IP address three suspicious situations can be identified according to Spam:

1. Calls from different domain and from the same IP address.
2. Calls from the same caller and from different IP addresses.
3. Different callers from same domain and from the same IP address.

Situation 1 gives the highest probability to be Spam. Situation 2, which could be legitimate in case of a mobile device or a dynamic IP address, gives a lower probability for Spam. Situation 3, which could be legitimate in case of Network Address Translation (NAT), gives the lowest probability for Spam.

Evaluation

These three cases do not give decisive information about the call being Spam or not, but it could give some information about the likeliness of the call being Spam. Although this countermeasure is very unreliable in an isolated form, it could give some hints in order to trigger other countermeasures.

5.1.8. Domains of Trust

For this approach every domain has a certain trust value in accordance with the likeliness Spam originating from this domain. The Trust Value is computed by means of some known security characteristics of that domain (e.g. identity strength and effectiveness of the implemented Spam countermeasures) and its historical behaviour. This method could be implemented by means of a central authority which issues certificates to all domains and verifies the security characteristics.

Evaluation

For the domains of trust approach there has to be a certain trust in the other networks or in the central authority. In order to define and test the security characteristics of the domain, there is a need for a reliable Spam detection mechanism and it requires cooperation of every domain owner. Security, and Spam in particular, must be part of the Service Level Agreement (or Interconnection Agreement) in order to ensure the cooperation of the interconnection partners.

In order to make an implementation, some standardization work has to be done. For a consistent assessment of the domains, the security characteristics have to be uniform and a clear process for measuring these characteristics is required. In case of implementation by means of a central authority, the communication between the domains and this authority has to be standardized.

5.1.9. Behaviour Analysis and Limitations

Caller's behaviour can be analysed using statistical metrics (e.g. call rates, spacing between calls, call duration, number of concurrent calls, etc.). With these metrics (i.e. features) some standard profile has to be defined according legitimate behaviour. The more the behaviour from a caller deviates from this profile the higher the probability for Spam. The aim is to identify anomalies and well-known Spam patterns. Behaviour analysis is often implemented by signalling protocol analysis (i.e. analysis of the information in the SIP headers).

The metrics can be divided into static and dynamic attributes. Static attributes are those attributes deduced from one single call (e.g. call duration). Attributes deduced from multiple calls are called dynamic attributes (e.g. call rate).

The list bellow contains attributes which can be defined in a behaviour analysis implementation. This is not a complete list of all attributes which are possible, but just a list of examples. *Chapter 6* provides more examples of attributes. The implemented attributes are a matter of need and taste.

- **Identity Strength** (static) – The amount of trust that can be placed in the user's ID. An strong identity is less likely to be (mis)used for Spamming.
- **Type of User** (static) – It is possible to define multiple user types (e.g. residential, enterprise, call centre), which have a different behaviour.

- **Cost of Call** (static) – The costs which have to be paid by the caller. More expensive calls are less likely to be Spam.
- **Call Duration** (static) – The duration of a call. Short, callee terminated calls are more likely to be Spam.
- **Callee Terminated** (static) – Whether the callee ended the call. Callee terminated calls are more likely to be Spam.
- **Connection Security** (static) – The amount of trust that can be placed in the connection security. A secure connection is less likely to be (mis)used for Spam.
- **Call Rate** (dynamic) – The amount of call attempts of one user/source in a certain timeframe. A source with a high call rate is more likely to be a Spam source.
- **Call Completion Rate** (dynamic) – The amount of initiated calls compared to the total amount of call attempts in a certain timeframe. A call attempt could, for instance, fail because the callee is unknown (i.e. the SIP response '404 Not Found' is sent back by the network). A poor call completion rate is an indicator for Spam.
- **Call Duration Consistency** (dynamic) – The variation in call duration. Less variation in call duration is more likely to be Spam.
- **Number of Unique Callees** (dynamic) – The amount of unique callees for one source in a certain time frame. A high amount of unique callees for one source is more likely to be Spam.
- **Number of Concurrent Calls** (dynamic) – The number of calls that are done in parallel. More than one or two concurrent calls are more likely to be Spam. For the implementation of this metric a clear definition of 'one call' is important. E.g. is a conferencing call always 'one call'? If a second call has been made after the first call has been placed on hold, is this still 'one call'?

Next to the possibility of analysing the attributes and comparing it with a 'legitimate profile', it is also possible to configure limits on these attribute. For instance, the end-user is allowed to initiate at most 8 phone calls every 60 seconds.

Behaviour analysis could be used as a defensive countermeasure. In this approach the analysis is used by the Spam prevention system for making decisions on what action to take for each call. It is, furthermore, possible to use behaviour analysis as a detective countermeasure and it can provide input for the monitoring approach.

Evaluation

The behaviour analysis approach seems to be a promising approach for counteracting VoIP Spam. The attributes could be measured relatively easy and discover extraordinary behaviour. However, it is difficult to classify extraordinary behaviour as being Spam. In a lot of cases it is impossible to take decisive choice according to behaviour, because it is impossible to embrace human behaviour in one (simple) model.

The model for legitimate behaviour should be made by means of real telephone data. In order to keep the 'legitimate' model accurate user feedback can be used for False Positives and False Negatives. In order to make the behaviour model we need a sufficient amount of data. Note that a call profile changes during a day, week, month, year, etc. *Figure 8* denotes the communication profiles for residential and enterprise users expressed in the number of call attempts during one hour. This information is extracted from a two-week traffic sample of Swisscom's VoIP network.

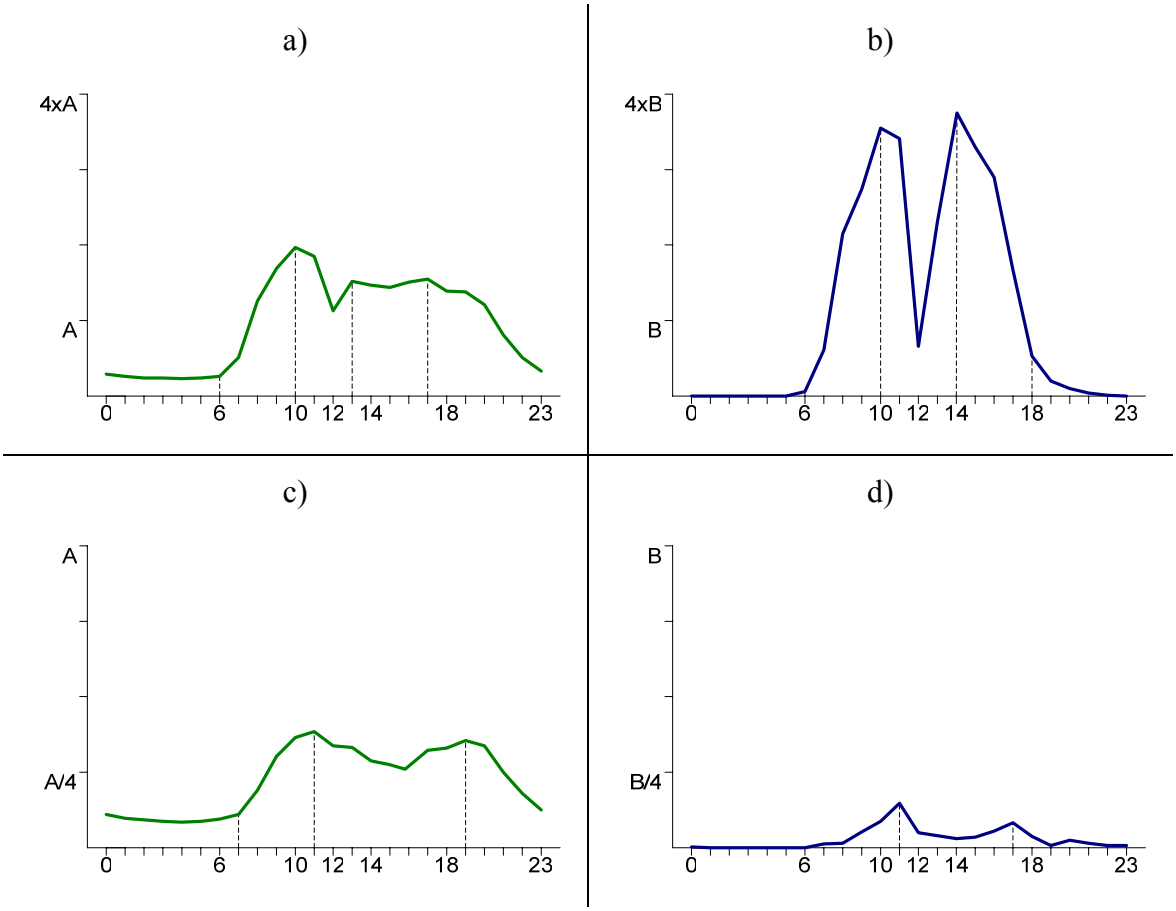

Figure 8: The number of call attempts in an hour during the week for residential a) and enterprise b) users and during the weekend for residential c) and enterprise d) users

In order to measure behaviour a strong identity is evidently needed. Without a strong identity it is impossible to measure behaviour of one originator and as a result the behaviour analysis approach will have limited effect.

Another difficulty is to distinguish between Spammers and active call centres. In a call centre it is very often the case that an Automatic Call Distributor (ACD) initiates calls and whenever a recipient picks up the phone the call is forwarded to an agent. Due to this principle the agents do not have to wait for the recipient to pick up the phone, but the behaviour of this ACD is somehow similar to the behaviour of a Spam machine. The ACD use statistical approach for the number of calls he initiates each second.

5.1.10. Reputation System

In this approach the users are able to give feedback on the communication they have with other users. After user A communicated with user B, user A gives a feedback value saying how satisfactory this communication was. All feedback from users on communication with user B gives information about the reputation of user B in this community. Every time a phone call is initiated the callee sees the reputation value of the caller and this can help him to take the phone call or not. A reputations system is also called a Web of Trust or a Social Network. There are several algorithms for the calculation of the reputation, for instance, the EigenTrust Algorithm [48].

An example of an implemented reputation system is eBay (www.ebay.com), which is a virtual market place where visitors can buy and sell products. On eBay, every seller has a reputation value saying the percentage of positive feedback on the transactions. An implementation of a reputation system in a VoIP infrastructure is described in [57].

Evaluation

A reputation system is a very complex approach for Spam prevention. The effectiveness of the approach is highly dependent on the end-user's cooperation. In big VoIP communities a reputation system requires a lot of storage and high computational power. In our opinion a reputation system for VoIP Spam prevention will only work in reasonable small communities. For larger (possibly worldwide) communities this approach is too complex, because trust between the VoIP networks is required. This is contradicting with the VoIP Spam problem, which only exists when the community is large enough.

There is a potential problem for identity misuse. Identities with a high reputation are attractive for misuse for Spam purposes. For the reputation system a strong identity is evidently needed. Without a strong identity the reputation values do not give any information of the likeliness of the call being Spam.

5.1.11. Consent-based Communication

With consent-based communication the consent of the recipient is required in order to initiate new communication. When the originator tries to initiates new communication, the recipient's consent is being asked by the system. The callee evaluates the call attempt by means of the information he received from the network (e.g. caller's ID). Only if the callee accepts the call, the call is established. A collect call is an example of consent-based communication. In this model the consent is not only asked for accepting the communication itself, but also for being charged for the communication. A framework for consent-based communication in SIP is identified in [46].

Evaluation

Consent-based communication could be annoying for legitimate users. If this countermeasure is implemented in an isolated form, every call attempt needs more effort than the users are used to in the PSTN. Like the Turing test, consent-based

communication should be used only as a backup countermeasure, which is activated in case other countermeasures do not give a decisive answer on the call being Spam or not.

5.1.12. Computational Intensive Puzzles

Before communication gets initiated the initiating device first has to solve a puzzle which requires (some) computational power. This way a Spamming machine could make less communication attempts in the same timeframe because of a delay caused by the puzzle. When the puzzle is simple enough, a legitimate user would not notice the delay. The puzzle could, for example, be implemented by a large arithmetic problem which must be solved by the originating device.

Evaluation

This countermeasure is not focussed on counteracting Spam, but the focus is on slowing down communication and thereby slowing down a Spam machine. In our opinion, this is not a proper way of preventing Spam. Although the end-user might not notice this puzzle, there is still a delay. It is likely that the legitimate user has a hard phone which has less computational power than a Spam machine or a Bot network. Since the price for computational power is decreasing, a perpetual adaptation of the puzzles is required.

5.1.13. Monitoring

A VoIP monitoring system scans the activities on the VoIP network and generates alarms at certain suspicious events (e.g. call rate of a user is above a certain threshold). Monitoring requires human judgement on extraordinary behaviour. For VoIP Spam prevention, a specialist should look into these events and take an appropriate action according to his observations. The methods used by Spammers as well as the Spam sources could be identified by monitoring.

A honeypot is a monitoring tool for attracting malicious activities in order to research the attacker's behaviour. In case of VoIP Spam this could be implemented in the following way: Some dedicated phone lines are configured to always answer and play a pre-recorded message. The activity on such a line is monitored and could result in information about Spammer's methods and Spam sources. Such a honeypot could also be used in order to prevent ID guessing, because random dialling will sooner or later end up in such a honeypot.

Evaluation

Monitoring is a tool to obtain information about Spamming behaviour on the network. This information is important in order to optimize implemented countermeasures. For effective monitoring end-to-end signalling encryption could be a problem, because the activity details (provided by signalling analysis) could not be observed. However, in most implementations the encryption is terminated at the entrance of the network.

An implementation of a monitoring system should be preceded by considering the (regional) law, because possibly legal boundaries exist for the use of monitoring. Content

analysis, for example, could provide legal problem in cases other than lawful interception. For the implementation of honeypot it should be clear how far one could go in attracting 'bad' behaviour.

Because spam is a worldwide problem rather than a local problem, sharing the knowledge among telephony providers is important.

5.1.14. User Defined Conditions

A user can define different policies and conditions for incoming phone calls. For instance, reject some type of phone calls in a certain time frame; apply a different set of countermeasures or a different strength of the countermeasures at certain times. As a result, a user could reflect his preferences, state of mind, or his presence on the defined conditions. *Table 11* denotes some examples of user defined conditions.

```
IF caller_group = black_list →
    block_without_message()


IF 00:00 < time < 06:00 →
    IF caller_group NOT IN (family, friends) →
        block_with_message('Sorry, we are not
        available at the moment')


IF 12:00 < time < 13:00 →
    IF caller_group = unknown →
        block_with_message('We are having lunch at
        the moment, please call back after 13:00')
    IF caller_group ≠ unknown →
        block_with_turing('We are having lunch at the
        moment, please call back after 13:00 or dial the
        following code in case of an urgent matter')
```

Table 11: Examples of user defined condition

This approach could also be used for parental control. Thus parents can define policies on their child's telephone access. For instance, no phone calls during the night.

Evaluation

User defined conditions is the first step to give the user freedom in configuring his telephone characteristics, which is in our opinion important. Although this approach does not directly counteract VoIP Spam, it could reduce the impact of VoIP Spam for the end-user.

The definition of conditions could be complex for some people. Therefore, the service provider could configure some default conditions which are useful for most users.

5.1.15. Multiple ID's

A user could have multiple ID's which he can use in different ways. For instance, a user has a main ID, which he only gives to people he trusts (i.e. family and friends), and one or more other ID's, which he can use for communication with people he does not trust or people with whom he has a short-term relationship (i.e. sellers, shops, etc.). Communication on these extra ID's is forwarded to the main ID. Once one of these extra ID's is filled with Spam a user could easily delete it. As a result, a user can keep his main ID Spam-free by not revealing it to untrusted parties. Since it has little impact for the user to change these extra ID's, it is less important to keep these ID's Spam-free.

This approach could also be extended by throw-away ID's or fake ID's. These ID's can be used for cases where a user has to enter his ID, but he doesn't want these people to have his ID. A nice example of a fake ID is the Frank-geht-ran service [49]. This service provides some phone numbers which are answered by the following message:

> *„Guten Tag liebe Anruferin, lieber Anrufer. Ich bin Frank und nehme im Auftrag Ihres erhofften Gesprächspartners diesen Anruf entgegen. Ich darf Ihnen ausrichten, dass eine telefonische Kommunikation nicht gewünscht ist. Daher bedaure ich sehr, die Verbindung nun trennen zu müssen."*

Evaluation

For the implementation of this approach, the user's cooperation is very important. The user has to use the ID's wisely; otherwise the effect on VoIP Spam is limited. For some users this approach could be complex. Although this approach does not directly counteract VoIP Spam, it could reduce the impact for the end-user.

It could be difficult for a user to keep the main ID private. This depends highly on the strictness of the user and the users he trusts to receive the main ID. It seems to be impossible to keep the main ID 'Spam free', but at least the amount of Spam on this main ID can be reduced. If only communication via the extra ID's is allowed, the main ID could be hidden for everyone and remain Spam-free regardless the user's method for using his extra ID's.

5.2. Legal Countermeasures

Anti Spam legislation [12][67] enables legal penalties for Spamming. Although some people judge legislation as not so efficient [Q 1.10], we think it is an important basis for efficiently counteracting VoIP Spam. If the penalty is high enough and the chance to get caught is also high enough, this will discourage people to Spam.

In order to make legislation effective, international cooperation between governments is required [47]. This is, however, a very difficult and expensive process. The definition for Spam for example is already very different between countries (*Section 4.9*).

In order to apply the legal penalties, a reliable method for Spam detection is required as well as a reliable method to prove Spamming behaviour. Technical countermeasures have to be used to detect VoIP and prosecute the Spammer. For proving Spamming behaviour, cooperation of the end-user (i.e. the victim) is required.

5.3. Social Countermeasures

Also on the social level VoIP Spam could be counteracted. In this section some social countermeasures are described which all have a preventive effect. Most people do not see social countermeasures as effective [Q 1.11]. However, the approaches in this section could be the starting point of further research.

5.3.1. Immediately Contact Originator

When Spamming behaviour is detected, the originator is contacted immediately by the service provider and asked to explain his action. This could discourage Spamming in a very early stage.

Evaluation

Due to anonymity of the originator it is in most cases impossible to contact the originator. Especially when the Spam is sent via a Bot network a legitimate user is contacted instead of the Spammer. Though, this could also help the legitimate user to become aware of his computer's infection. A service provider could help the customer with cleaning his device.

5.3.2. User Education

As in a lot of security issues the user is the weakest link also in the Spam problem. User education could help users to use their communication methods properly, in order to reduce the amount of Spam they receive and to stimulate the anti Spam offensive. The fields were users might need some education are:

- **How to recognize Spam?** – Only if the user could recognize Spam, he can react according to it.
- **How to react to Spam?** – Since the recipients who react keep the Spam problem alive, the main message to the user is 'Do Not React'. The recipient should know what the effect of reacting to Spam is and also what the effect of opting-out could be (see *Section 4.6.1*).
- **How to use credentials?** – The user should know how to use information such as username, SIP URI and password in order to prevent it from (mis)use. If the user

has multiple ID's (see *Section 5.1.15*), he should know how to use and separate these ID's.

- **What is done against Spam?** – The user should know what is done by the service provider to counteract Spam, in order to cooperate.

Evaluation

Since this countermeasure will only have effect if the majority of the users act accordingly, the implementation of this countermeasure seems to be complex and ineffective. In general it is difficult for users to act for the common good. However, user education could still improve the user's awareness and acceptance of implemented countermeasures.

5.3.3. Aggressive Spam Prevention

Aggressive Spam prevention is an approach for scaring off the Spammer from his business by scaring him or bringing him (financial) damage. This could be done in the form of counter attacks (e.g. 'Spam the Spammer' or DoS attack).

Evaluation

Next to the ethical and legal complaints against this approach, it is often difficult to identify the Spammer with a high certainty. When aggressive counter attacks are applied to the Spam source, it could harm a legitimate user in case of a Bot network (*Section 4.6.3*). There might be a potential for an 'arms race' when implementing this countermeasure.

5.4. Commercial Countermeasures

Since most Spammer seems to act from financial motivations, commercial countermeasures could be effective. One of the reasons why Spam is not a problem on the PSTN is the charge one has to pay for making telephone calls. The commercial countermeasures have a limited effect for the counteraction of Spam other than commercial and fraudulent. Also the questionnaire respondents identify the commercial countermeasures as being relatively helpful [Q 1.12]. Although the commercial countermeasures might counteract VoIP Spam, it could have an effect on the wide adoption of the VoIP technology.

5.4.1. No Free Calls

Every phone call costs a certain (small) amount of money for the originator. This way it is less attractive to use VoIP Spam for advertisements. This is similar to the current situation on the PSTN.

Evaluation

Since 'cheap telephony' is one of the key advantages for VoIP, the No Free Calls approach would slow down the widely acceptance of the VoIP technology.

5.4.2. Payment at Risk

Every time a call is established between the caller and the callee the caller immediately pays a certain (small) amount of money. Only if the user decides that the phone call was Spam, the caller loses his money, otherwise he gets his money back. This way it is less attractive to use VoIP Spam for advertisements. The money must go to a non-profit organisation; otherwise this will become a business model.

Evaluation

Although this approach is relative complex, it is better than the No Free Calls approach as regards user acceptance of VoIP.

Trust in the end-user is essential because the user's decision has direct financial consequences for the initiating party. When a callee does not like the callee he could bring him financial damage, regardless whether the communication was Spam or not.

5.5. Countermeasure Matrices

This section provides two matrices, i.e. *Table 12* and *Table 13*, with which the countermeasures can be compared. In both matrices the countermeasures on the left side are the identical to the ones described in *Section 5.1* till *Section 5.4*. This matrix is filled by our own judgement, thus the values are not absolute. Every value is dependent on the actual implementation and the values are very well debatable. However, this matrix gives a rough indication of the characteristics of the countermeasures.

Table 12 shows a matrix with all countermeasures mapped to the countermeasure classes (like explained in the introduction of this chapter) and the Spammer's methods (like explained in *Section 4.6*). The mapping between the countermeasures and the Spammer's methods is done by means of a value (i.e. -1, 0, and 1). -1 means that the countermeasure does not apply to the method. 0 means that the countermeasure could apply to the method in some circumstances. 1 means that the countermeasure applies to the method.

Table 13 shows a matrix with all countermeasures mapped to the inherent problems. The matrix identifies how the problems (see *Section 5.6*) apply to the countermeasures. The mapping between the countermeasures and the problems is done by means of a value (i.e. -1, 0, and 1). -1 means that the problem fully applies for the countermeasure. 0 means that the problem partly applies to the countermeasure (depending on the implementation and the system's environment). 1 means that the problem does not apply to the countermeasure.

For designing a Spam counteraction architecture this matrix could be used to determine the most preferred countermeasures. For this, prioritization of the methods and problems is required in order to calculate the effectiveness of a countermeasure.

1 Useful 0 Possible -1 Ineffective	Classes				Spammer's Methods					
	Preventive	**Defensive**	**Detective**		Advertising	Attracting	Impersonating	Behaviour Recording	Call-back Seduction	Terminating at Callee's Answer
Technical Countermeasures										
White Listing (private)		X			1	1	1	1	1	1
White Listing (group)		X			1	1	1	1	1	1
Black Listing (private)		X			1	1	1	1	1	1
Black Listing (group)		X			1	1	1	1	1	1
Gray Listing		X			1	1	1	1	1	1
Turing Test		X			1	1	1	1	1	1
Callee Feedback			X		1	1	1	1	-1	-1
Content Analysis			X		1	1	1	0	-1	-1
IP/Domain Correlation		X			1	1	1	1	1	1
Domain of Trust		X			1	1	1	1	1	1
Behaviour Analysis		X	X		1	1	1	1	1	1
Behaviour Limitations		X	X		1	1	1	1	1	1
Reputation System		X			1	1	1	1	-1	-1
Consent-based Communication	X				1	1	1	1	1	1
Computational Intensive Puzzles	X				1	1	1	1	1	1
Monitoring			X		1	1	1	1	1	1
User Defined Conditions	X				1	1	1	1	1	1
Multiple ID's	X				1	1	1	1	1	1
Legal Countermeasures										
Anti-Spam Legislation	X				1	1	0	1	0	0
Social Countermeasures										
Immediately Contact Originator	X				1	1	1	1	1	1
User Education	X				1	1	0	0	-1	-1
Aggressive Spam Prevention	X				1	1	1	1	1	1
Commercial Countermeasures										
No Free Calls	X				1	1	1	1	0	0
Payment at Risk	X				1	1	1	1	0	0

Table 12: Countermeasure applicability matrix

	Inherent Problems													
	Identity Misuse	Introduction Problem	Uncooperative end-users	Complex for (leg.) callers	Annoying for (leg.) callers	Annoying for callee	High Storage Demands	Computational Intensive	Dep. On Spam Detection	(Media) Encryption	Complex implementation	Legal limitations	False Negatives	False Positives
Technical Countermeasures														
White Listing (private)	-1	-1	-1	1	1	1	0	1	1	1	1	1	-1	1
White Listing (group)	-1	-1	0	1	1	1	0	1	1	1	1	1	0	0
Black Listing (private)	-1	1	-1	1	1	1	0	1	1	1	1	1	1	-1
Black Listing (group)	-1	1	1	1	1	1	0	1	-1	1	1	1	0	-1
Gray Listing	-1	1	1	1	1	1	0	1	-1	1	1	1	0	0
Turing Test	1	1	1	-1	-1	1	1	0	1	1	0	1	1	1
Callee Feedback	-1	1	-1	1	1	1	0	1	1	1	0	1	1	-1
Content Analysis	1	1	1	1	1	1	-1	-1	1	-1	0	-1	1	1
IP/Domain Correlation	1	1	1	1	1	1	1	1	1	1	1	1	-1	-1
Domain of Trust	1	1	1	1	1	1	1	1	0	1	0	1	0	0
Behaviour Analysis	-1	1	1	1	1	1	0	0	1	1	1	1	0	0
Behaviour Limitations	-1	1	1	1	1	1	0	0	1	1	1	1	0	0
Reputation System	-1	-1	-1	1	1	1	0	1	1	1	0	1	0	0
Consent-based Communication	-1	1	1	1	-1	-1	1	1	1	1	0	1	1	1
Computational Intensive Puzzles	1	1	1	1	0	1	1	0	1	1	1	1	-1	-1
Monitoring	1	1	1	1	1	1	-1	1	1	-1	0	-1	1	1
User Defined Conditions	1	1	1	-1	1	1	0	1	1	1	1	1	1	1
Multiple ID's	1	1	-1	-1	1	0	1	1	1	1	1	1	1	1
Legal Countermeasures														
Anti-Spam Legislation	1	1	0	1	1	1	1	1	-1	1	1	1	1	1
Social Countermeasures														
Immediately Contact Originator	-1	1	1	1	0	1	1	1	-1	1	1	1	1	1
User Education	1	1	-1	1	1	1	1	1	1	1	0	1	1	1
Aggressive Spam Prevention	-1	1	1	1	-1	1	1	1	1	1	1	1	1	1
Commercial Countermeasures														
No Free Calls	-1	1	1	1	1	1	1	1	1	1	1	1	1	1
Payment at Risk	-1	1	-1	1	1	1	1	1	-1	1	-1	1	1	1

1 Positive
0 Medium
-1 Negative

Table 13: Countermeasure problem matrix

5.6. Countermeasure Problems

In the evaluation of the countermeasures provided in this chapter as well as in the countermeasure matrix (Section 5.5) a set of problems is used. In this section some of the more important ones are explained in more detail. It is assumed that the rest of the problems are clear from the name only.

5.6.1. Identity Misuse

For the most countermeasures a strong identity is evidently needed, because there is a potential for identity misuse. A strong identity embraces both a difficulty for spoofing an identity and for obtaining a fresh identity. A strong identity makes it possible to trace people and to watch their behaviour. A strong identity could also be seen as a countermeasure in the sense that it becomes easier to counteract VoIP Spam

For the PSTN, telephony authentication was not an issue before, because the user was identified by the line (i.e. the physical location is known). However, if the user is connected via a mobile endpoint (or has a nomadic behaviour), of which the physical location is not known, identification (and thereby authentication) becomes a bigger and more difficult issue. The location of VoIP endpoints are in most implementations not known (or there is an uncertainty), thus authentication is the key factor.

Section 7.1.2 provides more information on how to improve the identity strength.

5.6.2. Introduction Problem

This problem occurs while using a white list or a reputation system for countering VoIP Spam. The question here is how to deal with ‘good guys’ who are not yet on the list; i.e. how a new user (or a user with a new identity) could be introduced on such a system. Other countermeasures could be used in order to add users to these lists. A couple of examples are mentioned in Section 5.9.

5.6.3. High Storage Demand

Especially the countermeasures which maintain lists of users with user characteristics have a storage demand. Since the price of storage is nowadays decreasing, this requirement is seen as a little investment. However, a high storage demand also implies more processing time for storing and recovering information. The storage requirement of a countermeasure depends on the community size.

5.6.4. Computational Intensive

Some countermeasures require high computational power. Therefore, more expensive hardware is required in order to implement the countermeasure. Implementations of countermeasures which require high computational power on hardware with a lack of

computational power could cause delays. Furthermore, these systems are vulnerable for DoS attacks.

5.7. Acting on Spam Detection

It is important to take appropriate action in a Spam prevention model. When one or multiple countermeasure modules identify the likeliness of the call being Spam high enough the following actions could be used:

- **Mark the Call** – The call is marked with a value which gives the callee information on the likeliness of the call being Spam.
- **Generate Alarm** – An alarm is generated and the action is stored for further (human) analysis, e.g. by the network administrator.
- **Inform Users** – All users of the VoIP network are informed in order to be aware of the Spam attack.
- **Filter Tuning** – The information is used to update the VoIP Spam prevention system.
- **Apply Other Countermeasures** – Other (stronger) countermeasures are applied. This approach could be used in situation when it is not possible to make a decisive choice.
- **Redirect the Call** – The call is redirected to another phone number.
- **Spam Voicemail** – The call is redirected to a special voicemail box, dedicated for Spam messages. In this approach a recipient is still able to listen to the Spam messages and the False Negatives.
- **Block the Call** – The call initialisation does not succeed. Blocking could be done by a hard block (i.e. a SIP error message is sent back) or a polite block (i.e. a message is played with the reason for blocking and/or instructions for contact at a later time or via another channel).
- **Reshape the Users Connection** – The usage of the user's connection is limited. I.e. the user could make less phone calls or use less bandwidth.
- **Block the User** – The user is unable to make any more phone calls. This could be done for a short term (i.e. between 1 minute and 1 day) or a long term (i.e. more than 1 day or the user has to contact customer care in order to unblock his telephone access).

In all these scenarios it is important to reveal as little information as possible to the Spammer about the action. It is a preferred situation that a (Spam) machine can not distinguish between a successful Spam call or a block/redirected call. As a result, less information about the anti Spam mechanism is revealed, thus for the Spammer it becomes more difficult to tune his machine in order to bypass the anti Spam mechanisms. Another requirement is that the ability to reach emergency services may never be affected by these actions.

If it is chosen to block a user at a certain point this should be done in a proper way, though this should only be done in extreme cases. Since it might be the case that a user is infected by a virus which is causing the Spam being sent, the service provider should help the user if he is blocked. For example, the user who is blocked could hear the following message at each call attempt:

> *"We're sorry, but we cannot put you through. Your device is exhibiting unexpected behaviour. Your device could be infected by a virus. Please contact the Swisscom helpdesk, number 0900 1234, or by pressing 1."*

5.8. Spam Prevention and Network Architecture

In VoIP Spam prevention an important issue is where to place the anti VoIP Spam modules in the network architecture. This question seems to boil down to the question where to place a certain (technical) countermeasure in the network architecture. Every countermeasure has its own preferred location. Some countermeasures you would place at the originating side and others on the terminating side.

	Network-based	Recipient-based
White Listing (private)		X
White Listing (group)	X	
Black Listing (private)		X
Black Listing (group)	X	
Gray Listing	X	
Turing Test	X	X
Callee Feedback	X	X
Content Analysis	X	
IP/Domain Correlation	X	
Domain of Trust	X	
Behaviour Analysis	X	
Behaviour Limitations	X	
Reputation System	X	X
Consent-based Communication	X	X
Computational Intensive Puzzles	X	
Monitoring	X	
User Defined Policies		X
Multiple ID's		X

Table 14: The place of technical countermeasures in the network

In order to fit the countermeasures into a network architecture, a distinction between network-based and recipient-based countermeasures can be made. A network-based countermeasure, which can be seen as a network defending mechanism, is applied inside the network and affects multiple users. A recipient-based countermeasure, which can be seen as user feature, is applied at the terminating side of the network or on the user's device and affects only one user. A recipient-based countermeasure should be configured by the user and a network-based countermeasure should be configured by the network owner. A private white list is a pure recipient-based countermeasure as a Turing test could be both. *Table 14* gives a global overview whether the technical countermeasures explained in *Section 5.1* can be used network-based or recipient-based.

In this research it is chosen not to go deeply into the topic of Spam counteraction architectures . This topic could be used for further research and probably it should be investigated at the time a specific Spam prevention model is being implemented.

5.9. Possible Countermeasure Combinations

Like stated in the introduction of *Chapter 5,* combination is the key. In this section some possible combination are described. This is by far not a complete list of all possible combination, but some simple combinations are listed.

5.9.1. White list and others

In order to reduce the size of the list the white listing approach should be combined with other countermeasures. A white list is an excellent countermeasure to combine with any other countermeasures. In such a combination you identify the caller which can bypass the Spam prevention system by means of a white list.

5.9.2. Black list, White list and Behaviour Analysis

The behaviour of callers is measured with the aim to take smart decisions according to this analysis. The callers on the white list are able to pass always and the callers on the black list are blocked always. The unknown callers are verified by behaviour analysis.

5.9.3. White list and Turing Test

Combining a white list with a Turing test is a closed approach in which everyone who is not on the white list must perform a Turing test. Although this approach is too annoying for normal use, it can very well be used in a company environment. In this model only (known) customers are directly connected to the callee and all others get, for example, a IVR menu. Also for children's phones this approach could be favourable.

5.9.4. Payment system with implicit Reputation values

An idea for a payment system of which reputation values can be derived is explained in [57]. In this model the recipient decides the fee for the call and the call is only initiated, if the caller accepts this fee. From these payments reputation value can be deduced.

5.9.5. Multiple ID's and User Defined Conditions

A user can have multiple ID's which all have different policies. As a result, the user is able to use different ID's for different roles which might require different communication patterns. For example, a user could define a business ID, which he uses for work related communication, and a personal ID, which he only use for communication with family and friends.

Chapter 6
Anti VoIP Spam Products

On the Internet, Jack reads about some companies which have implemented anti VoIP Spam techniques. He tries to find out what kind of mechanisms they use to counteract Spam. Once again he tunes his system to handle these products.

To be continued…

Currently, multiple companies are developing anti VoIP Spam products. The list bellow gives an indication of the work being done. The information is obtained by means of product evaluation (the software of NEC Corporation, Eyeball Networks, the University of Potsdam) and product descriptions on the suppliers' websites and product sheets (the other software).

- **VoIP SEAL (NEC Corporation)** – NEC's VoIP SEAL is a piece of software built upon SIP Express Router (SER), which is an open source SIP server. The software uses a two step model [56]. At the time of writing, the first step is implemented by a couple of modules (i.e. black/white list (*Section 5.1.1* and *Section 5.1.2*), call rate limit (*Section 5.1.9*), and IP/domain correlation (*Section 5.1.7*)) which give a Spam score. For this Spam score an upper and a lower threshold is configured. If the score is below the lower threshold, the call is initiated. If the score is above the upper threshold, the call is blocked. If the call is in the 'grey area' between the upper and the lower threshold, the call is redirected to the second step. This second step is implemented by a Turing test. *Section 6.2* provides an evaluation on NEC's software.
- **Eyeball Anti-SPIT Server (Eyeball Networks)** – Eyeball has built their patent-pending Anti-SPIT technology, specified in [55], in an extra module for their SIP proxy server. This module implements some hard limits (e.g. call rate limit, unique recipient limit) and some soft limits (e.g. short calls, unknown callees) by means of a dynamic scoring system. A high Spam score implies a decrease of the call rate limit. *Section 6.1* provides an evaluation on Eyeball's software.
- **Anti-SPIT System (Toplink GmbH)** – Toplink claims to have an anti VoIP Spam system which limits the amount of calls a caller can make [51].
- **VoIP Anti-Spam (Sipera Systems)** – Sipera claims to have an anti VoIP Spam technology based on policy filtering, behaviour learning, and Turing tests [73]. They built this technology into their IP Communication Security (IPCS) products.

- **SIPassure (Borderware Technologies Inc.)** – Borderware claims to have an anti Spam filter in their Session Border Controllor (SBC) product. "SIPassure protects against application specific threats including spam and connection (or call) flooding." [52]. The product uses anti Spam policy rules, white lists, and black lists in order to counteract VoIP Spam. Furthermore, SIPassure uses the Borderware Security Network (BSN) to identify Spam attacks and sources. All installed Borderware products provide information about the attacks to the BSN.
- **ETM Voice IPS (SecureLogix)** – SecureLogix sells the ETM Voice Intrusion Prevention System (IPS), which aims to counteract VoIP Spam and other threats. "The ETM Voice IPS applications provides real-time protection and prevention of threatening or abusive call patterns including VoIP Spam" [53]. Most probably they use behaviour analysis (*Section 5.1.9*) to detect abusive call patterns.
- **Spam Prevention System (SPS) (Voice & Data Security Solutions)** – Voice & Data Security Solutions (VoDaSec) claims to have the solution for VoIP Spam. Their SPS technology should be able to "detect any voice Spamming effort within a shortest possible time without maintaining any state about the caller or performing any lookup into a database" [54]. In their approach they use behaviour analysis (*Section 5.1.9*) to detect Spamming behaviour by using a selection of the signalling information.
- **VoIPblock (VoIPshield)** – VoIPshield's VoIPblock is an anti VoIP Spam system that can be used on an IP PBX, softswitch, or SBC product. On their website [81], they claim that the product embraces white and black lists, user feedback functions and a correlation engine. What exactly the meaning is of this correlation engine is not clear.
- **Anti-SPIT Software (University of Potsdam)** – The University of Potsdam has developed a Java software package for VoIP Spam counteraction. This software embraces thirteen modules which are mainly based on white/black listing and caller behaviour. For this research we reviewed the software for evaluation, which is described in *Section 6.3*.

6.1. Eyeball's Anti-SPIT Server

Eyeball Networks has developed a patent-pending Anti-SPIT technology which is fully compliant with SIP based VoIP environments. Basically this technology boils down to limit the number of calls a caller can initiate as well as callees can receive. Also a couple of other limits are incorporated.

For this research we evaluated Eyeball Anti-SPIT Server software. For the evaluation the software was installed on the CentOS 5 distribution of Linux according to the installation manual. After installation the software was configured being the proxy server for our SAP Spam source (*Appendix B*). The evaluation is done on both the functioning of the implemented countermeasures and the configuration of these countermeasures.

According to the manual the following features are implemented in this software:

1. **Call Rate Limit** – The number of calls a user can initiate in one time frame.
2. **Unique Callee Limit** – The number of unique contacts a caller can phone in one year.
3. **Unknown Callee Penalty** – When calls are initiated to 'unknown' callees, the call rate limit is decreased.
4. **Short Call Penalty** – When a 'short' call is terminated by the callee, the call rate limit is decreased.
5. **SPIT Report Penalty** – When VoIP Spam is reported, the call rate limit is decreased.
6. **Recovery** – How fast the call rate limit will increase (after a penalty) to reach its original value again.

These features form an implementation of the behaviour limitation (*Section 5.1.9*) approach. In Eyeball's white paper about this anti VoIP technique [55] it is also mentioned that also the caller's reputation is important, but we could not find this in the product manual nor in the software itself.

After evaluation of the different features we composed the following findings about the six features mentioned before:

1. **Call Rate Limit** – It is possible to configure the number of calls and the time frame. When the call rate limit is set to x it is possible to make x/2-1 phone calls in the same time frame. When the call rate limit is exceeded the calls are blocked. Most probably the reason that it is only possible to make x/2-1 phone calls is that for every phone call two INVITE requests are sent and every INVITE request is counted as one phone call by the software.
2. **Unique Callee Limit** – When the callee limit is set to x it is possible to make calls to x-1 unique callees. When the x^{th} call is being initiated this call and all the next calls are blocked.
3. **Unknown Callee Penalty** – The Unknown Callee Penalty feature could not be tested, because it was not clear what an 'unknown' callee is. Most probably the SIP response '404 Not Found' is used as indicator.
4. **Short Call Penalty** – We could not get the Short Call Penalty feature working.
5. **SPIT Report Penalty** – The SPIT Report Penalty feature could not be tested, because it was not clear how to 'report' VoIP Spam.
6. **Recovery** – We could not get the Recovery feature working.

The system-wide configuration of the limits and penalties is possible via a database or via a Command Line Interface (CLI). It is not possible for the individual users to reflect their preferences onto the system in the sense of configuration. This contradicts with the idea

of the client-side parental control function, which Eyeball mentions in their white paper [55].

Another point is that it is impossible to see the current status of the Anti-SPIT modules (e.g. the current Call Rate Limit of a user). Furthermore it is impossible to change the action which is taken whenever the call rate limit is exceeded. The calls are always blocked in case the Call Rate Limit exceeds, but in some cases it is better to redirect the phone calls or to apply stronger countermeasures.

To conclude this evaluation, in our opinion the philosophy of the anti VoIP Spam technology is good because the dynamic call rate system limits exceptional behaviour and is not noticeable for normal users. However, we missed easy configuration, status information and action configuration. It could be the case that we evaluated the software in a wrong way and overlooked some things. Since Eyeball was not willing to give us feedback on the outcomes, it was not possible to verify our method of working.

6.2. NEC's VoIP SEAL

Note: The text in this section has been reviewed by NEC and publication is permitted.

NEC Corporation has developed a product for VoIP Spam counteraction, namely VoIP SEAL. VoIP SEAL is based on the SIP Express Router (SER) [74], which is a multifunctional SIP server (i.e. registrar, proxy, and redirect server). NEC's software is an implementation of the two-step model [56], like depicted in *Figure 9*. The two-step model implements the anti VoIP Spam countermeasures into two different stages. In the first stage multiple modules (i.e. countermeasures) are executed in parallel and provide information on the likeliness of the call being Spam. The second stage module is only for the cases where it is impossible to make a decisive choice.

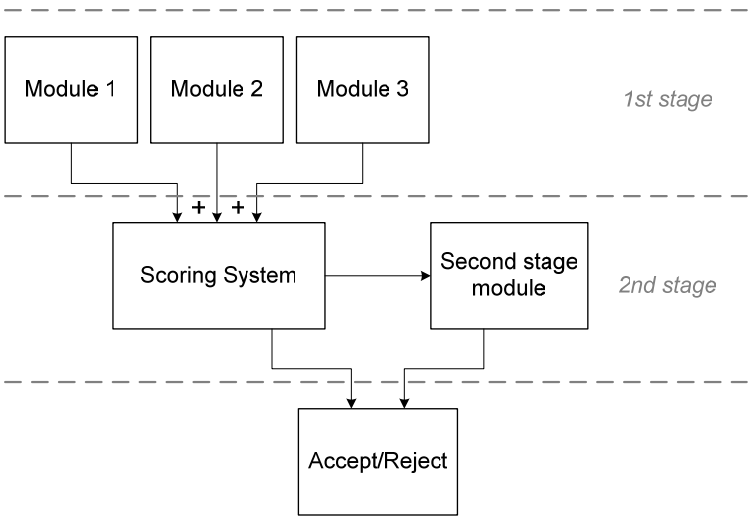

Figure 9: Two-step model

For this research NEC offered a test version of VoIP SEAL. This test version was installed on a Debian Linux 4.11 host and configured being the proxy server for our SAP Spam source (*Appendix B*). The evaluation is done on both the functioning of the implemented countermeasures and the configuration of these countermeasures. The information in this section is based on this evaluation version. By the time of reading specific details could have been changed, because NEC is working very intensively to improve the software.

In SER's configuration it is possible to define routing logic for incoming messages. NEC uses this routing logic to route the INVITE requests to VoIP SEAL. Subsequent to the INVITE's arrival it is forwarded to the first stage. All the first stage modules are executed in parallel and return a score value which ranges from 0 to 1 (from -1 to 1 for the list module) and is used to calculate the total score value. In our evaluation version the following first stage modules are implemented:

- **Black/white list** – This module returns a score value 1 if the caller's ID is on the black list, -1 if the caller's ID is on the white list, and 0 if the caller's ID is on none of these lists. See *Section 5.1.1* and *Section 5.1.2* for more information about white lists and black lists.
- **Call Rate** – For this module the values `period`, `threshold` and `maximum` are configured. The value `calls` is defined to be the number of INVITE messages that are received by VoIP SEAL during the last `period` seconds. The score value of this module is calculated by the following formula:

$$\mathrm{MAX}(\mathrm{MIN}(\ \frac{\texttt{calls} - \texttt{threshold}}{\texttt{maximum} - \texttt{threshold}}\ , 1), 0)$$

  Figure 10 depicts the relation between `calls` and the score value for this module, when `threshold` is configured to be 2 and `maximum` to be 6.

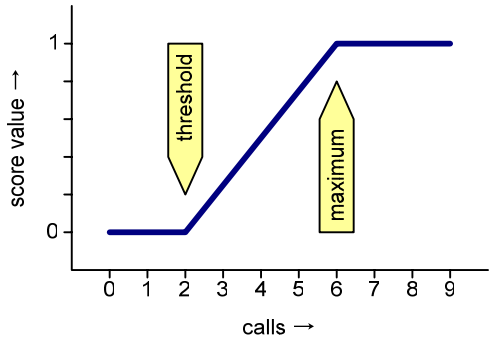

Figure 10: Increase of the Score Value for the Call Rate Module

(`threshold`=2, `maximum`=6)

  This implementation of behaviour limitation (see *Section 5.1.9*) is in our opinion very favourable, because it is possible to configure a soft limit (i.e. `maximum` > `threshold`) instead of a hard limit (i.e. `maximum` = `threshold`).

- **IP/Domain Correlation** – This countermeasure is explained in *Section 5.1.7*. If case 1 (see *Section 5.1.7*) is detected, then the score value is defined to be 0.25. If case 2 (see *Section 5.1.7*) is detected, then the score value is 0.15. If case 3 (see *Section 5.1.7*) is detected, then the score value is 0.05.
- **Simultaneous** – If multiple calls are executed in parallel, then the score value is non zero. 2 simultaneous calls results in the score value 0.25. 3 simultaneous calls results in the score value 0.5. More than 3 simultaneous calls results in the score value 1.0. This is another implementation of behaviour limitation (see *Section 5.1.9*). *Figure 11* depicts the relation between the number of simultaneous calls and the score value of this module.

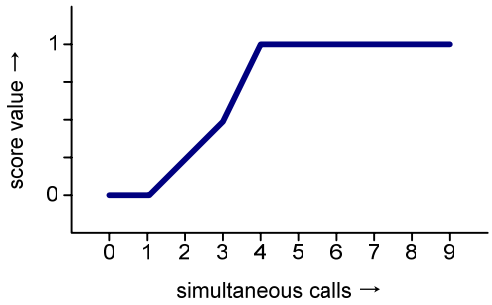

Figure 11: Increase of the Score Value for the Simultaneous Module

- **Dummy** – This module returns always the score value 0.25. This module is implemented for test purposes and can be used to increase the total score value with a fixed value.

For every module a weight value can be configured. The total score value is the sum of the products of every score value and its corresponding weight. There is an upper and a lower threshold for the total score value configured. If the total score value is bellow the lower threshold, than the call is initiated. If the total score value is above the upper threshold, then the call is blocked. If the total score value is between the two thresholds, then the call is forwarded to the second stage.

The second stage is implemented by means of a Turing test (call pattern observation, see *Section 5.1.4*). As soon as the caller ends up in the Turing test a message is played to him. Only if there is no (reasonable) speaking activity during this period, the call is initiated.

NEC's software architecture is straightforward and modular. The different modules can be switched on/off and the influence of the modules can be altered by means of the weight values. Since the software is based on SER, which is licensed under open-source GNU license, the system is flexible and transparent.

The software version which we used for the evaluation was equipped with a Graphical User Interface (GUI, see *Figure 12*) and multiple logging tools. As a result, it was easy to obtain status and behaviour information.

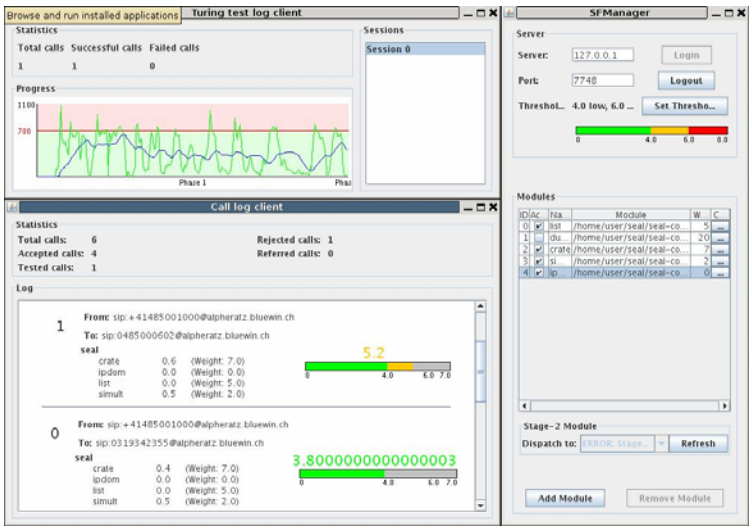

Figure 12: GUI of NEC's VoIP SEAL

Another positive point is that NEC is currently active in some IETF drafts in the field of VoIP Spam (see *Chapter 10*). As a result the potential standards are very likely to be incorporated into NEC's VoIP SEAL.

In contrast to the software from Eyeball (see *Section 6.1*), we think that NEC's software has the potential to become a serious weapon against VoIP Spam. The modular structure makes the software very flexible and ready for extensions in the future. However, we define a couple of points for improvement.

- **Simultaneous Module Configuration** – In the evaluated implementation the values used to determine the score value for the simultaneous module are not configurable. We would recommend the same configuration method (i.e. threshold and maximum) as is used for the call rate module. NEC points out that in the current release they already implemented configuration options for the simultaneous module.
- **Individual Configuration / Group-wise Configuration** – In the current implementation only system-wide configuration is possible. In our opinion it is preferable to have the possibility to make a configuration profile per user or per user group according to their requirements. There is, for example, a significant difference in requirements for residential users and for enterprise users. More variety makes it also more difficult for a Spammer to adjust his Spam system to bypass the filter. NEC points out that user or group customization is the target for further releases. As a result, a distinction can be made between residential and enterprise users.
- **Turing Test** – In our opinion, the current implementation of the Turing test would have limited effect on counteracting VoIP Spam. It is very easy for a Spam machine to wait for silence before starting to play the Spam message. A voice interpretation challenge or a simple puzzle (see *Section 5.1.4*) would have more effect, but these are, of course, more annoying for the caller. NEC points out that in the current release they have implemented two new stage-two modules. One

Turing test which asks the caller to give random input (see *Section 5.1.4*) and one that asks the caller to call back at a later time (see *Section 5.7*).

NEC points out that they are currently working on the integration with proxy servers other than SER. NEC's long term view is to have a distributed solution with the modules scattered across the network.

6.3. Potsdam University's anti SPIT Software

Note: The text in this section has been reviewed by the University of Potsdam and publication is permitted.

The Institute for Computer Science at the University of Potsdam (Germany) has implemented algorithms to detect VoIP Spam. For this research we obtained the software from the University of Potsdam in order to evaluate it. Due to the late arrival of this software, it could not be implemented in our SPIT Analysis Platform. The evaluation described in this section is done by means of source code analysis.

The software package, which is written in Java, implements a score rating system in which the score value is calculated by means of thirteen modules. Every module can be used as recipient-based or network-based countermeasure and returns a score value which ranges from 0 to 1. The total Spam score, which expresses the likeliness of the call being Spam, is calculated by means of the (weighted) score values of the modules. The following modules are implemented:

- **System White List** – This module returns a score value 0 if the caller's ID is on the system white list and 1 if it is not on this list. This system white list module is an implementation of a group white list (see *Section 5.1.1*).
- **White List** – This module returns a score value 0 if the caller's ID is on the white list of the callee and 1 if it is not on this list. This white list module is an implementation of a private white list (see *Section 5.1.1*).
- **Black List** – This module returns a score value 1 if the caller's ID is on the black list of the callee and 0 if it is not on this list. This black list module is an implementation of a private black list (see *Section 5.1.2*)
- **Misdialled Calls** – This module measures the number of misdialled calls (i.e. calls to callees which are not known by the system) in the last 24 hours. This module returns a score value 0 in case of nine or less misdialled calls and 1 in case of ten or more misdialled calls (see *Figure 13*).

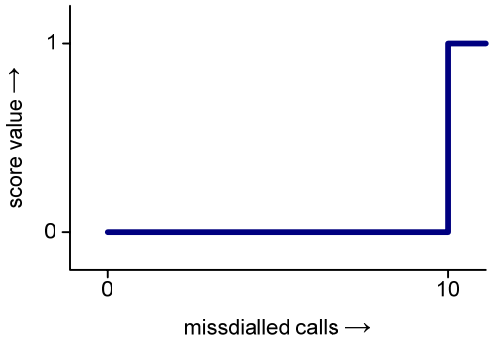

Figure 13: Number of misdialled calls mapped onto the score value

- **Concurrent Calls** – This module measures the amount of calls that one caller initiates in parallel. The number of concurrent calls in measured by counting the calls a caller initiates within the same 10 seconds. *Figure 14* shows the mapping of the number of concurrent calls onto the score value.

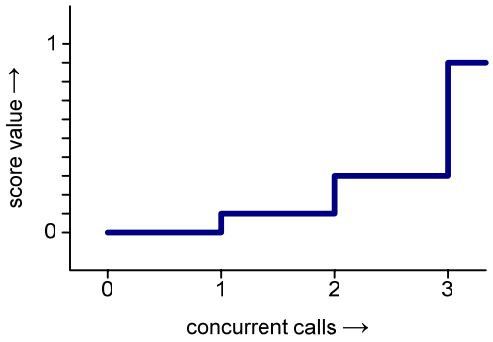

Figure 14: The number of concurrent calls mapped onto the score value

- **Call Trend** – This module compares the number of calls a caller has initiated during the last 12 hours with the number of calls initiated during the preceding 12 hours. A trend ratio is calculated by the following formula:

$$\frac{\texttt{calls\_this\_interval}}{\texttt{calls\_previous\_interval}}$$

In this formula `calls_this_interval` is defined to be the number of calls in the last 12 hours and `calls_previous_interval` the number of calls in the preceding 12 hours. *Figure 15* shows mapping of the trend ratio onto the score value.

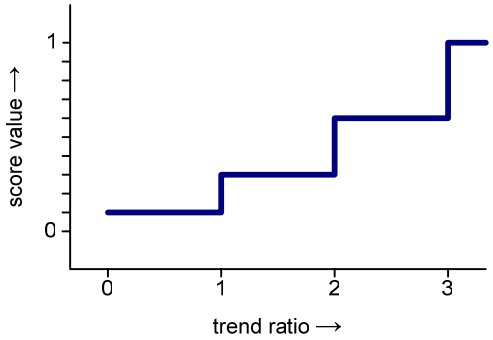

Figure 15: Trend ratio mapped onto the score value

- **Call Breadth** – This module measures the relation between the number of calls and the number of distinct callees. The score value of this module is calculated by the following formula:

$$\frac{\texttt{distinct\_callees}}{\texttt{calls}}$$

  In this formula `calls` is defined to be the number of calls initiated by the caller and `distinct_callees` the number of distinct callees in these calls. As a result, the score value ranges from 0 to 1 ($0 < \text{score value} \leq 1$). For instance, if all calls are initiated to unique callees, then the call breadth is maximal and the score value is 1.

- **Call Proportion** – This module compares the amount of calls a caller initiates with the average call proportion of all users on the system. A proportion ratio is calculated by the following formula:

$$\frac{\texttt{calls}}{\texttt{total\_calls / users}}$$

  In this formula `calls` is defined to be the number of calls initiated by the caller, `total_calls` the number of calls initiated on the system, and `users` the number of users on the system. *Figure 16* shows how the proportion ratio is mapped onto the score value

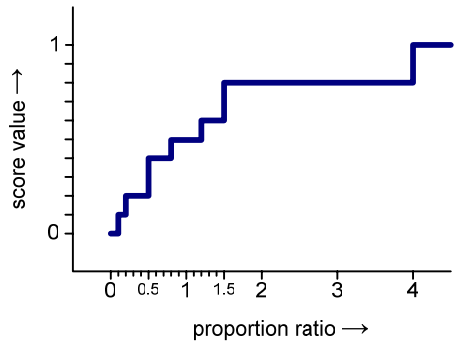

Figure 16: Proportion ratio mapped onto the score value

- **Provider Prognosis** – This module extracts the score value from a header in the INVITE message. This module can be used as a recipient-based countermeasure in order to extract the Spam score calculated by means of the network-based countermeasures. More information on communicating the Spam score via a SIP header can be found in [82].
- **Call Back** – This module checks whether the callee has initiated communication to the caller in the past. If the caller is once called by the callee, then the score value of this module is 0. If not, then the score value is 1.
- **Reputation** – This module calculates the reputation of the caller. A reputation value is the average Spam rating of the caller's communication attempts in the past. The score value of this module is equal to the reputation value. See [57] for more information about the reputation system used.
- **Rejected Payment** – The software implements a payment system in which the caller has to pay an amount of money according to the Spam score of the call. The caller can decide to accept or reject the payment. This module counts the amount of payments which are not accepted by the caller in the last 24 hours. *Figure 17* shows the mapping of the number of rejected payments onto the score value.

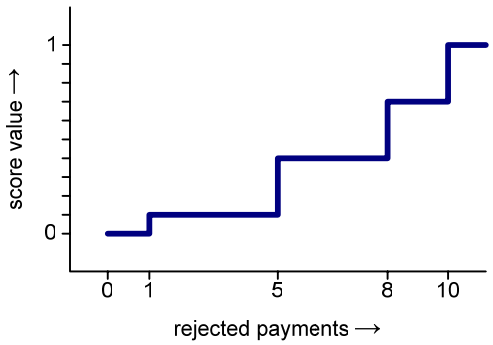

Figure 17: The number of rejected payments mapped onto the score value

- **System Spam Ratio** – The system stores the information of every phone call together with the corresponding Spam score. This module gives the proportion of calls that have a Spam score of 0.8 or higher. The score value is calculated by the following formula:

$$\frac{\texttt{spam\_calls}}{\texttt{total\_calls}}$$

In this formula `total_calls` is defined to be the number of calls initiated on the system and `spam_calls` the number calls initiated on the system with a Spam rate of 0.8 or more. As a result the score value ranges from 0 to 1 ($0 <$ score value ≤ 1). For instance, if all calls have a score rate of 0.8 or higher, then the Spam ratio is maximal and the score value is 1.

For performance reasons the modules are used in different levels. In every level one or more modules are executed and produce a Spam score. Only if no decisive choice can be made after a level is the next level executed. In which level a module is used is dependant on the module's decisiveness and the required computational power. At the time of writing three levels are implemented in the software package. The first level checks the white list. If the white list module gives a positive score (i.e. 0), then the call is accepted. If the white list gives a negative score (i.e. 1), then the call is processed by the second level. The second level is implemented by means of the black list. If the black list module gives a negative score, then the call is rejected. If the black list module gives a positive score then the call is processed by the third level, in which all the other modules are used and a weighted average of all score values is returned.

The code analysis gave us a good impression of the software. In our opinion the code is well written and has a potential to become the basis of a stable and reliable proxy module. For the mappings onto the score values the consistency was not completely clear. However, the software authors explained to us that the current mappings are the result of intuition and experience. They are planning to improve the mappings by means of tests with real telephony data.

The software authors also have an ongoing discussion about further mechanisms to prevent VoIP Spam. Currently further research is done in the following fields: content analysis, address obfuscation, moderation, computational puzzles, Turing tests, legal action and time conditions. However, in their point of view these approaches cannot be used to prevent VoIP Spam during call initiation.

Chapter 7
Countermeasure Design

***Illustration**: After 4 months of Spamming, Jack notices that some of the service providers he has used for Spamming are implementing countermeasures for VoIP Spam. Due to his former research into the possible countermeasures and the enhancements of his Spam system, he can handle most of the techniques. However, the toughest problem for him is that the service providers have enabled a wide range of possibilities for user customization. As a result, Jack experiences the complexity of programming his Spam machine to handle all the different configuration users can have. The users who use a turing test are now completely unreachable for him.*

To be continued…

In this chapter the aim is to identify how the VoIP Spam problem must be tackled. The model for VoIP Spam counteraction is not static; it should be adjusted as time goes by, the VoIP Spam problem unfolds, and more knowledge and real examples are available in this field. This chapter only embraces a high level description of a VoIP Spam prevention model. For the implementation and configuration the specific needs of residential and enterprise users and their distinct behaviour must be taken into account.

For the professional Spammer, Spam is (just) a way of earning a living. Thus, he will invest a lot to protect his income, but the question is what maximum investment the Spammer is willing to make. It is easier to discourage people who are just starting to Spam via VoIP. If we act now, it will be less attractive for E-mail Spammers to change over to VoIP Spam.

In *Chapter 5* and in the Spam literature the main focus of Spam counteraction is on increasing the Spammer's investment. This usually comes down to preventing Spam messages from arriving at the recipient. In *Section 7.1* a model for increasing the Spammer's investment is explained. Although increasing the Spammer's investment is a good and respected approach for Spam counteraction, there is also another approach which in our opinion could provide possibilities, namely decreasing the Spammer's benefits. This approach requires further research, but some ideas are explained in *Section 7.2*.

7.1. Increase the Spammer's Investment

None of the countermeasures, provided in *Chapter 5*, will be perfect in isolated form, therefore combination is the key. The countermeasures should be combined in such a way that they are most effective in counteracting VoIP Spam without being a hindrance for the end user. In our opinion user control on the countermeasures is clearly required, in order to avoid user resistance and to give the user freedom. Individual configuration of the anti VoIP Spam mechanism makes it also more difficult for a machine to Spam, because there are a rich variety of manners a call is handled. The implemented countermeasures should not be a hindrance to the user, but should be presented as extra functionality.

VoIP Spam could slow down the wide acceptance of the VoIP technology. However, a bad implementation of an anti Spam technique could also deter users. This is especially the case when those countermeasures are used which require a cooperative user. All telephony users in the PSTN are used to a certain degree of service quality and they are not willing to accept less when they switch to a new technology. Since they expect this new technology to provide advantages in all fields, all implemented countermeasures should be either invisible for the user or enable new functionality.

Furthermore, the countermeasure model must be flexible and modular in order to enable easy modification in the future. Since the way how the VoIP Spam problem will evolve is not predictable, it should be taken into account that the future possibly requires changes in the implemented modules or requires extra modules to be implemented.

In this section we describe our preferred model for increasing the Spammer's investment, which is meant to be used in the next couple of years (i.e. 2008, 2009 …). We expect that the VoIP Spam problem is not yet going to be unfolded completely in these years. These years might be the time in which both the Spammers and the users discover the VoIP Spam phenomenon. Implementing this model would discourage VoIP Spam already in an early phase.

Our investment increasing model is three fold:

- **User Portal** – The user portal gives the users the opportunity to express their preferences and needs according to their telephony service. As a result users could easily avoid receiving unsolicited phone calls.
- **Strong Identity** – A strong identity is essential for the counteraction of VoIP Spam. As described in *Chapter 5* a lot of the countermeasures' effectiveness is dependent on the strength of the identity. Nomadic behaviour requires a stronger identity than currently is implemented in most VoIP networks.
- **Monitoring** – Since VoIP Spam is not yet a problem, the evolvement of the phenomenon should be tracked by means of monitoring the network. Especially honeypots are a promising method for gathering information about VoIP Spam attacks.

In *Section 7.1.1*, *Section 7.1.2*, and *Section 7.1.3* these parts are explained in more detail.

IETF's Internet Draft on VoIP Spam [1] identifies four important recommendations for VoIP Spam counteraction: (1) Strong Identity; (2) Use White Lists; (3) Solve the Introduction Problem; and (4) Don't Wait Until its Too Late. The countermeasure model provided in this chapter complies with these recommendations, but is a more extended and complete approach.

If there is a need for more countermeasures in the future, an more extended architecture should be developed in which different countermeasures can be implemented in a modular way. At the time of writing, a promising architecture is the two-step model [56], which is the basis for NEC's VoIP SEAL (see *Section 6.2*).

7.1.1. User Portal

Users should be able to use a user portal (i.e. web-application) in order to configure their telephone service. For the sake of VoIP Spam counteraction this user portal must give the user the ability to configure different recipient-based countermeasures (see *Section 5.8*). Furthermore, a user must be able to see which calls were blocked by the anti VoIP Spam mechanism and add the caller's ID to the white list in case of a False Negative.

The user portal must be easy to use and provide the users with full freedom for their telephony service. The service provider must enable a standard configuration profile for users for whom it is difficult to manage their telephony service by means of a user portal. User education (*Section 5.3.2*) is important in order to minimize the FRR and the FAR by means of the configuration in the user portal.

The following features must be available for the user in order to counteract VoIP Spam:

- **Address Book combined with Group-based Forwarding** – A user is able to add contacts to the address book and sort them into groups. For every group the user can define a forwarding rule (e.g. redirecting, bypass filter, blocking). As a result, a user has white/black list functionality (see *Section 5.1.1* and *Section 5.1.2*).
- **Call Logs** – A user can see the incoming and outgoing calls with the corresponding information (e.g. originator). It is possible to mark a call as Spam in order to provide feedback to the service provider or add the caller's ID to the address book.
- **Time Conditions** – A user can define time conditions in order to apply different configuration at different time frames. For instance, only callers who are in some specified groups of the address book (e.g. family and friends) can initiate calls during the night.
- **Spam Filter** – If one or more network-based countermeasures (see *Section 5.8*) are implemented, a user is able to configure the security level. For example, if this Spam counteraction system outputs a percentage expressing the likeliness of the call being Spam, the user could define a threshold for the calls which should be redirected to the Spam voicemail. The configuration for enterprise users could be

more extensive (e.g. threshold: 0%-100%) than the configuration for the residential user (e.g. levels: low/medium/high).

- **Spam Voicemail** – The phone calls which are identified being Spam should be forwarded to the Spam voicemail. This voicemail's inbox should have an E-mail-inbox-like interface in order to scan and delete the messages easily.
- **Digital Receptionist** – A user is able to define an audio message which is played at certain events and which might requires user input. A combination with the time conditions is preferred. A user could, for example, enable the following message during lunch time: "*We are currently having lunch, please call back after 13:30 or dial 468 in case of an urgent matter*". This is an example of a Turing test (see *Section 5.1.4*).

In order to implement these features, a technique for policy based forwarding is required. A start has been made for standardizing policy techniques for SIP [77]. An advanced user (e.g. enterprise user) might be able to make some customized policies in order to enable some specific conditions. Also policies for parental control would be very helpful in order to prevent children from receiving (harmful) Spam messages.

If the multiple ID's approach (see *Section 5.1.15*) is implemented, the user portal could be used to manage these ID's.

7.1.2. Strong Identity

As explained in *Section 5.6.1* strong identities are essential for multiple countermeasures. In some VoIP networks the user subscription is bound to a physical access line, because the user is only allowed or able to initiate phone calls from his home network. Thus, the identity is reasonable strong and comparable to the identity strength in the PSTN. The authentication in most SIP environments is done by the digest access authentication method which is specified in [63]. This is a challenge-response mechanism and is based on the MD5 hash algorithm.

In many VoIP networks the password (i.e. the secret) is known by the user and often the user can change it. This has, of course, impact on the strength of the secret. Storing the secret on a digital media (e.g. smart card, memory card, USB flash drive) rather than in the user's brain would enable longer and more random passwords. In cellular telephony the secret is stored inside the SIM on the Universal Integrated Circuit Card (UICC), which is a removable smart card. This principle can also be used for VoIP telephony. 3GPP made a standard for an IP multimedia Subscriber Identity Module (ISIM) on a UICC for IMS [10]. The ISIM contains the secret and other information to register on the VoIP network. Since hard phones with smart card readers are currently rare and the use of smartcards is only standardized for IMS, it is currently difficult to implement it in broad extend.

For the future, when the user is more mobile and the access point is not 'known' or not trusted than other methods for authentication are required. Authentication must be done by means of certificates issued by the service provider to customers after a signed

contract together with a copy of the customer's passport is submitted. A certificate would enable foreign networks to authenticate users in a secure way without connecting to the home network. Certificates give the user more freedom for checking the identity and the service provider's identity of the origin.

7.1.3. Monitoring

In our opinion monitoring is important. Monitoring could give information on how the VoIP problem is evolving and which methods the Spammers are using. Monitoring is important in order to 'know the enemy' and to fine tune the implemented preventive and defensive countermeasures.

Monitoring could be done by one or more of the following approaches:

- **Behaviour Analysis** – The activity on the VoIP network is logged and the user's behaviour is compared to a legitimate behaviour profile (see *Section 5.1.9*).
- **Honeypot** – Multiple ID's are configured to terminate on a machine configured to answer all communication and records caller's behaviour. The aim is to attract Spammers in a subtle way and to gather information on the attacks and the sources. The recordings can also be used as proof for Spamming behaviour.
- **Callee Feedback** – Users who receive Spam give feedback to the service provider. This feedback is stored by the service provider for further analysis or for gathering proof.

A monitoring system should generate alarms in case of extraordinary behaviour of its users. Human interference might be needed in order to analyse the events. In case of legitimate behaviour, one might want to tune the monitoring system. In case of Spamming behaviour appropriate steps are required. Possible actions are described in *Section 5.7*. These actions are, however, only possible if the Spam originates from the service provider's network. If the Spam originates from another network, then this network's owner should be contacted and the information about the attack and its origin should be delivered.

A honeypot could cause legal problems, because it attracts illegal behaviour. There might be a problem with recording communication on this honeypot. However, this honeypot could be compared to a voicemail box and for every call which terminates on this honeypot the following message is played: "*The phone number you have dialled does not exists, please dial again. Your communication is being recorded*.". In the case of monitoring by means of a honeypot the local laws should be studied in order determine which recording methods are legal and which not.

7.2. Decrease the Spammer's Benefits

Next to increasing the Spammer's investment we could also try to decrease the Spammer's benefits. Since the main motivation for Spammer's is commercially oriented, the success-rate (i.e. the proportion of recipients that react) is the Spammer's key factor for success (in terms of benefits).

Our goal is to prevent the user from reacting to Spam, thus we have to define what kind of reaction we want to avoid. The first aim of a Spammer is to initialize the phone call and he wants the phone call to be answered. The avoidance of these reactions is covered by the model for increasing the Spammer's investment, like discussed in *Section 7.1*. For commercial and fraudulent Spam most of the Spam messages are furthermore aimed to sell products or to generate hits (on a website). The avoidance of these reactions is discussed in this section.

The Spam problem exists because of the recipient's reaction; if no recipient reacts to Spam, there would be no benefit for the Spammer. Decreasing the success-rate implies decreasing the Spammer's benefits. In order to decrease the success-rate two strategies are possible: (1) make sure the recipients DO not react; (2) make sure the recipients CAN not react.

In order to make sure that the recipients **do not react** to Spam, user education is essential. The users have to know that reacting on Spam will not only satisfy their own needs, but reacting on Spam will also contribute to the global Spam problem. Two things are important for the user to learn. Firstly, the user should be able to identify Spam messages and assess the validity of the information. Secondly, a user who wants to buy a product which is recommended by Spam should not use the reaction link provided in the Spam message. Though, users are commonly lazy and it is difficult for the user to behave for the common good.

Another approach is to make sure the recipients **can not react**, which is less dependent on user cooperation. At first sight this approach may be impossible to realise, but in our opinion there are possibilities in this field. In order to prevent users from reacting a service provider should be both able (in technical terms) to do so and allowed (in legal terms) to do so.

The first step in the technical realisation of the reaction-prevention mechanism is to maintain a (black) list of reaction links (i.e. HTTP URI's, SIP URI's, etc.) occurring in VoIP Spam messages. This list is the basis for a reaction-prevention mechanism and should be shared among interconnection partners. Maintaining this list could be done by means of a honeypot which attracts VoIP Spam attacks and records the Spam messages. The messages have to be analysed (by a human or a machine) in order to extract the link information.

The second step in the technical realisation is to either block these links for users, or warn them if they follow the link. Although the blocking approach could limit the user's freedom, in case of a phishing attack this could prevent the user from financial damage. The VoIP Spam message is received by means of a VoIP network, but the reaction path could require the use of a different communication channel (e.g. the web). In case of a HTTP link (i.e. a URL) in the VoIP Spam message cooperation with the user's ISP is required in order to prevent the user from following this link.

The legal realisation of the reaction-prevention mechanism is twofold: (1) legal authorization is required for recording Spam message in order to extract the reaction link from it; and (2) legal authorization is required for interfering with the recipient's reaction.

The reaction-prevention approach is an example of 'regulation by means of technology' which can create some resistance, but opinions can change on this. It might be an outrageous idea, but in our opinion it could provide possibilities for the future. An evaluation platform should be built in order to research this approach in more detail.

Chapter 8
Recommendations

***Illustration**: As soon as Jack discovered the SIP Broker website he can send Spam to networks he has not registered with. As a result, he can bypass the countermeasures more efficiently and extend the geographical range of his Spam action.*

To be continued…

This chapter provides recommendations in the field of VoIP Spam, supplementary to the recommendations in *Chapter 7*. Currently the VoIP Spam problem is not yet unfolded, thus it is not necessary to implement advanced and expensive countermeasures at the time of writing. However, a service provider must consider the problem while designing new telephony systems. The service provider must also follow the evolvement of the VoIP Spam problem and define clear security procedure for Spam incidents.

Since Spam is a worldwide problem rather than a local problem, worldwide cooperation between service providers is required. One part of this cooperation is to exchange information about Spam attacks and sources. An other part is to cooperate in standardizing the counteraction of VoIP Spam, in order to improve interoperability between the VoIP networks.

Before implementing VoIP Spam counteraction techniques, the (anti) Spam legislation in the concerning regions should be considered, because the law could have limitations for Spam prevention (see *Section 4.9.2*).

Since the different Spam problems (e.g. VoIP Spam, E-mail Spam, etc.) have similarities, cooperation between these different fields of research is favourable.

Chapter 9
Related Works

***Illustration**: Since the standards bodies are now active in the field of VoIP Spam, Jack foresees a more consistent implementation of the countermeasure which would cause big problems for his Spam machine.*

To be continued…

Since the beginning of the year 2007 some standards bodies have been active in the field of VoIP Spam in order to define the problem and standardize the countermeasures. The IETF initiated a couple of Internet Draft on VoIP Spam in the first half of 2007:

- Signalling TO Prevent SPIT Reference Scenario (11 January 2007) [27].
- SIP Extensions for SPIT identification (23 February 2007) [26].
- Authorization Policies for Preventing SPIT (26 February 2007) [77].
- A Framework for Reducing Spam for Internet Telephony (14 June 2007) [18].
- The Session Initiation Protocol (SIP) and Spam (9 July 2007) [1].

Also other standards bodies are publishing documents related to VoIP Spam: ETSI-TISPAN (Draft ETSI TR) and ITU (Draft Recommendations X.ocsip, X.fcsip and X.csreq).

Some of the companies stated in *Chapter 6* are also active in the field of VoIP Spam research.

Also work has been done on the VoIP protocols themselves, in order to make them more Spam resistant. A proposal to change SIP into the Differential SIP (DSIP) is described in [78].

Chapter 10
Further Research

***Illustration**: Now because of the higher investment Jack has to make in order to send VoIP Spam he thinks about using other techniques than only simple calling. Some of the VoIP networks he is connected to have a conferencing server. He creates another account on some of these networks. If he starts a conference with this account and invites the account of the Spam machine together with some other account he is still able to send effective Spam. This method gives him an extra advantage, namely that he only needs one audio stream for reaching multiple recipient, so he can make more Spam with less bandwidth.*

To be continued…

Since this research was limited in time, not every topic could be studied in great detail. In this chapter some ideas for further research are pointed out.

The model for decreasing the Spammer's benefits should be studied in more detail in order to disclose the possibilities of this approach. A test platform could provide more information about the performance of this model. Research on the user acceptance of such an approach should also be done.

Since Bot networks are the main source for Spam (at least for E-mail Spam), further research in this area is necessary. Currently there are a number of different research approaches in the field of Bot networks (see *Section 4.6.3*).

Honeypots are currently a respected way of researching security topics. Also Bot networks could be researched by means of honeypots. Next to the research capabilities of a honeypot, it could also be used for monitoring to provide information on current VoIP Spam attacks and proof. The application of honeypots in the field of VoIP is relatively new and further research is needed into this field before implementation is possible. However, there are already research activities in this field [76].

In this research the focus was on VoIP Spam by means of audio based phone calls, but also other kinds of spam are possible in a VoIP network (e.g. Video Spam, Conference Spam, and Text Message Spam). Although a lot of counteract approaches in this report are also applicable for other types of Spam in VoIP, these types could require some slightly different approaches in counteracting it. These types of Spam require research,

because they can provide possibilities for Spammers. In particular Conference Spam might be a big threat, because only one audio stream is needed from the Spam source into the network and still multiple recipient are reached. In addition, the initiator of the conference call might be distinct from the Spammer.

Research in the behaviour profiles for legitimate and postulate communication is required in order to implement an anti Spam model based on behaviour analysis or limitations.

In *Section 5.8* there are a few words on the preferred place for the countermeasures in the network architecture. This topic requires, however, further research in order to create an effective architecture for the anti VoIP Spam system.

Chapter 11
Conclusion

***Illustration**: Jack is required to continue the enhancements of his Spam system in order to maintain his income from VoIP Spam. This requires a lot of his free time, it tires him out, and also his wife is upset because he spends too much time in his study…*

As we have seen the Spam problem exists due to the fact that the costs (i.e. time and money) for the Spammer are far lower than the recipient's costs. The Spammer's total costs are his investment minus his benefits. Thus, in order to increase the Spammer's costs either his investment should be increased or his benefits should be decreased. Increasing the Spammer's investment boils down to preventing the Spam messages from arriving at the recipient's side. Decreasing the Spammer's benefits boils down to preventing the recipient from reacting to the message.

In this research we investigated the until recently non existing VoIP Spam problem. We expect that the coming few years the VoIP problem is going to unfold. Both, the Spammer and the legitimate user, will discover the VoIP Spam phenomenon in these years. If service providers act on in an early phase, they could prevent the VoIP Spam problem from growing into the problem E-mail Spam is today. For the service provider there are possibilities in counteracting VoIP Spam by increasing the Spammer's investment and there might be possibilities in decreasing the Spammer's benefits.

The characteristics of VoIP makes Spam on this communication channel more difficult to tackle. In addition, Spam via VoIP is more intrusive than Spam via E-mail, because VoIP is a real-time communication medium. We found a wide range of countermeasures of which only few provide realistic possibilities for the VoIP service provider. By building the analysis platform (see *Appendix B*) we have seen that sending Spam is easy, while counteracting it is far more difficult.

Three anti VoIP Spam products have been evaluated in this research, namely Eyeball's Anti-SPIT Server (*Section 6.1*), NEC's VoIP SEAL (*Section 6.2*) and anti VoIP Spam software from the University of Potsdam (*Section 6.3*). The latter two are promising approaches for VoIP Spam counteraction, due to the modular structure and thus the flexibility.

The service provider should cooperate with other parties in the field of VoIP Spam prevention. This cooperation is needed in order to (1) exchange information on VoIP Spam attacks and sources and (2) standardize techniques to counteract VoIP Spam.

By means of the model for decreasing the Spammer's benefits (see *Section 7.2*) the service provider is able to prevent users from reacting to phishing attacks. Due to a monitoring system the VoIP Spam attacks should be analysed and the reaction links which are used for the phishing attacks should be extracted. The service provider could inform the user about the attack or interfere with the user's reaction.

For the years coming in which the VoIP Spam problem is unfolding, the user's ability to act on personal Spam problems is important. In these years the user should be able to use countermeasures like black/white listing, user defined conditions, Turing tests and multiple ID's to counteract VoIP Spam. Next to the counteractive possibilities of these functions, they also provide favourable features for the user. The portal described in *Section 7.1.1* is based on these recipient-based countermeasures.

Next to the user's ability to counteract VoIP Spam, the service provider should monitor the network in order to 'know the enemy' and implement appropriate countermeasures when necessary. It is essential that the service provider acts immediately, because it is easier to counteract Spam in a very early phase. Once the amount of Spam grows due to bad implementation of countermeasures, it will be more difficult to reduce the amount of Spam then if appropriate countermeasures has been implemented right from the start.

Appendix A Questionnaire

This appendix contains the Questionnaire which has been used for this research and the response of 40 (anonymous) persons. Most of the respondents work in a telecommunication environment, but all work in different fields of expertise.

- 28 respondents work for Swisscom (Network Development, Innovations, Legal, Marketing, etc.)
- 9 respondents work for telecommunication suppliers of which 2 are active in the field of VoIP Spam
- 2 respondents work for telecommunication regulators. Respondent 29 works for BAKOM and respondent 38 works for OPTA.
- 1 respondent is finishing his Information Security Master's course.

Whenever the questionnaire feedback is used in this document a reference format is used as described in *Section 1.1*.

The following sections contain the questionnaire responses by means of an numbered list. The responses are intentionally left in the original form and no single corrections are applied.

A.1. General Questions

A.1.1. What is your definition of VoIP Spam?

1. VoIP Spam are messages delivered via electronic means, normally mass sendings that I, as receiver, have not requested and that bloc, degrade or hinder my VoIP Service. Normally the content is advertisement. .
2. unwished mass phone calls on VoIP
3. Unerwünschte Anrufe
4. Broadcasting of unsolicited voice messages
5. Unsolicited commercial calls, market research, also "information" about products or services which I have not asked for
6. Un welcomed calls from anybody especially tele marketing calls
7. malicious or bothering messages. I do not see commercial adverisments as spam (as long as I can restrict myself this messages
8. Masses of unwanted calls, annoying me and making my voice mail box worthless. However, if I carefully think about it: All kind of calls I didn't ask for (except calls from people I have a personal relation to; note that also such calls may be unwanted, but I woulld not call such calls Spam) . Already today there are Spam calls annoying me: Calls from marketing survey companies, calls from telephone companies, calls people selling magazines, … but luckily, in my case such calls are quite seldom (maybe because I reject anonymous calls and do not take all calls with numbers I don't know and because they never leave messages at voice maillbox
9. Unsolicited or unwanted com via Voip channel. In 99 I did highjacking Call centers with bots. A lot of fun with a a massive dialing power and unlimited access to a pbx functionality. Yes It was me who brought down VCIC in 20 seconds with artificial life bots, and yes they took over session of human agents as an accidental side effect. Fun time! Today this is much easier due to SIP to build mass outbound botnetworks if ouy have the knowhow and and security is sloppy. Skype API's controlled by bots to access gateways for woip spaming are probable but not very likely, due to inbuild mitigation, as far as I know.
10. For me SPIT is an overspecification of the problem. I would rather consider "Spam over Telephony". If it is over VoIP or not is actually not relevant. (in the same direction that customers don't care what thechnology they are using, they just want to place

aphone call). In that context, SPT is unsollicited and sometimes aggressive and/or deceptful commercial calls which purpose is to advertise, sell, close a contract, incite to call back, or perform a study. SPT can be performed life or through a recorded message. The calee can either be a person or a recording device (Combox). It may also include other form of communication based on existing telephony networks, like SMS (written or text-to-speech)

11. Calls with faked A-Number (caller-Number), SMS to the FIxnet Phone
12. ungewünschet Anrufe, Werbung, Textmessages
13. Unsolicited commercial and non-commercial calls on my VoIP telephony service.
14. Unerwünschte Anrufe (z.B. von MArketing Firmen, Meinungsforschung etc.)
15. Fully-automated, scripted direct marketing calls performed by TTS and AVR systems.
16. Automated, uninvited bulk messages (broadcast) which can be based on a marketing campaign (commercial) or with a suspect or "joky" background. The goal could be to entice to do call on a toll number or to disturb the customer (nigth time). Other attacker cases might be - flooding voice box; diversify of the content (integrity); tamper of DNS queries (DNSSEC for ENUM).
17. Basically, every unwanted received call from a person or system where no previous relationship (commercial or private) existed if a certain threshold of no. of calls is exceeded. This is regardless if the calling party is faked or not. (Note: this threshold may be zero if a user marked it's phone number in the public directory accordingly)
18. VoIP Spam is similar to email spam threat, unsolicited messages were distributed over a VoIP infrastructure. The different between email and VoIP SPAM is the medium. In email SPAM you can do content filtering and SPAM rating in advance before delivering the mail to the destinator. In VoIP SPAM content filtering is not possible because of real-time media. When your phone rings, it is already too late to prevent you from SPAM or SPIT (SPAM over Internet Telephony) so the preventing technique must be more elaborated than in the email-world.
19. USA defines it as tele-marketing. All telephone based un-wanted calls are defined as a SPAM. The US congress pass a low that allows end-user to put themselves on a 'do not call' list. The violators are fined by law.
20. Unsolicited, unwanted messages that are retrieved via VOIP
21. SPIT: massive, unsolicited VoIP-traffic, which is generally undesired. Disturbance of privacy.
22. Any undesired kind of calls(video, voice) [/chat/messages] with the intend to advertize for something or to request answers for sureveys.e.g. from call centers
23. Unerwünschte Anrufe auf meinen Telefonanschluss . Gleiche wie beim E-Mail aber auf dem Telefonanaschluss
24. Unsolicited calls
25.
26. http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-04.txt. Since SIP covers a broad range of functionality, there appear to be three related but different manifestations:
    Call Spam: This type of spam is defined as a bulk unsolicited set of session initiation attempts (i.e., INVITE requests), attempting to establish a voice, video, instant messaging or other type of communications session. If the user should answer, the spammer proceeds to relay their message over the real time media. This is the classic telemarketer spam, applied to SIP.
    IM Spam: This type of spam is similar to email. It is defined as a bulk unsolicited set of instant messages, whose content contains the message that the spammer is seeking to convey. IM spam is most naturally sent using the SIP MESSAGE request. However, any other request which causes content to automatically appear on the user's display will also suffice. That might include INVITE requests with large Subject headers (since the Subject is sometimes rendered to the user), or INVITE requests with text or HTML bodies.
    Presence Spam: This type of spam is similar to IM spam. It is defined as a bulk unsolicited set of presence requests (i.e., SUBSCRIBE requests for the presence event package), in an attempt to get on the "buddy list" or "white list" of a user in order to send them IM or initiate other forms of communications.
27. Unwanted VoIP communication attempts.
28. Anrufe / Aktionen, die ausschliesslichen Verkaufs- oder Störhintergrund haben (oder zumindest dies nich klar auszuschliessen ist) und zum Teil als automatisierte "Massensendungen" abgewicklet werden.
29. Über VoIP automatisch erzeugte Werbeanrufe, bei denen dem Angerufenen eine aufgezeichnete Werbebotschaft abgespielt wird. Werbeanrufe von realen Personen, die live am Telefon sind, gelten nicht als SPIT. Hingegen gilt als es unlautere Massenwerbung, wenn ein Call Center mehr Anrufe gleichzeitig tätigt, als Personen im Call Center verfügbar sind. (Dies wird im Ausland oft gemacht um die Call Center auszulasten, da in der Regel nur jeder zweite Angerufene antwortet. Heben dann aber doch einmal zu viele ab, wird den Überzähligen ein Warteband eingespielt. Dies wird vom BAKOM ebenfalls als unlautere Massenwerbung und damit als illegal taxiert.)
30. seen from the individual receiver: receive calls where the caller is not a human being, receive calls from from people/organisations trying to sell something during night time and repeated reception of calls from the same person/org. trying to sell the same thing over and over again
    seen globally: produce the above towards thousands of callees
31. VoIP Spam is: the transmission of unsolicited automated messages either directly to a VoIP subscriber actively 'listening' on the service; the deposit of an automated message in the subscribers Voice Mail box; or the indirect targetting of a vulnerability in a VoIP service to deposit a unsolicited message to a subscriber.
32. Repeated unwanted mass phone calls during daytime to sell products, to make fraud attempts, betrayal, especially in the residential area, targetting elderly people and housewifes. In the evening, calls can be targeted at young active urbans trying to sell other type of products. Spam can also be initated by bored hackers willing to seam anarchy and chaos, "just for fun"..
33. Unerwüschte Calls; Werbeanrufe; Anrufe von Computern, die feststellen ob jemand abnimmt ……
34. From a user point-of-view : getting (massive) unwanted media calls (audio/video).
35. This would be the same analogy as telemarketing calls in the TDM world.
36. receiving of unsolicited calls - calls I never ever wanted to receive
37. Meine Telefonie-Daten werden für den Versand von Telefoniespezifischen Werbungen verwendet. Beispiel: Ich werde von Brokern kontaktiert, welche spezielle VoIP Angebote vertreiben.
38. As a regulator OPTA is bound by leagal defiitions. Please refer to article .. of directive 2002/58 for the exact wording of the European ant-spam legislation. OPTA defines spam as any message or call anything that is sent or placed in contradiction with this legislation.

39. Unaufgeforderte Mitteilungen über VoIP (gleich wie E-Mail nur über Sprache..)
40. VoIP Spam is unsolicited commercial phone calls, or rather speaking of unsolicited bulk phone calls (similar to spam definitions in e-mail). This can include automatic, by robots initiated phone calls but also human-initiated calls. If we open up the scope we can also include other means of communication like texts being displayed on a phone (e.g. sms, e-mail). I also see a possible dimension of VoIP Spam in regard to filling up a user's voice mailbox up with advertisements as we know it from e-mail spam. I would not in clude attacks like phishing (social engineering) or trojans, viruses, buffer overflows etc. using VoIP into a VoIP spam definition.

A.1.2. Do you think that telephony emergency broadcasts are also Spam?

1. No, My Answer is towfold. I would consider your example as VoIP Spam, but in general "telephony emergency broadcast" as a service which I pay for, as in the TDM environment e.g. Pikettaufgebot für Feuerwehr
2. Yes, TV and newspapers are the right medium for that
3. No, Ich weiss nicht was ein telephony emergency broadcast ist. Falls es das ist , was ich denke: nein
4. Yes, If anyone can for any reason broadcast VoIP messages it is from my point of view spam.
5. Yes, This will be abused for "hidden" commercial calls. Since I spend my days in a different city I have a very low probability of helping, so this call just wastes my time.
6. Yes, There are enough other communication cannels like journals, radio and tv.
7. No, To me this is neither malicious nor bothering
8. Yes, If I go with the definition above it is spam. Of course it's for a very good reason, but it's still spam. But if the only reasons to get spam are missing kids then (I guess) most people wouldn't be annoyed.
9. Yes, DON'T: that is like ringing +41 *
10. Yes, I expect a phone call to be a unicast, from one person to another. It is not appropriate to use it as broadcast or as a mean to access many people in an undiscernable way over a short period of time.
11. Yes
12. Yes, Anrufe auf irgend ein Endgerät bringt doch nichts. Solche Suchen müssen gezielt geführt werden.
13. No, Depending on the situation, but normally not spam as the emergency broadcast are because of an emergency I should probably know about or can even help.
14. Yes, Ja. (Eine entsprechende Umfrage etc. wäre Aufgabe der Behörden (Polizei etc.) nicht von Privatpersonen.
15. Yes, Spam is communication you do not want to receive. If there would be a central office that asks people to subscribe to those calls (so those people accept these kind of calls), this communication would NOT be spam - if not, it is.
16. Yes, Because, it is a question how people communicate. If you publish such a headline in a newspaper or on television, that's not a personified message. However, a telephony emergency broadcast by using SPIT - all callees are involed even they know nothing about the disappearance of my kid..
17. Yes, Exception: If these calls are authorized by the government by law and only a public institutiion will place these calls.
18. No, In Germany no telephony emergency broadcasts systems exists in the traditional circuit switched telephony system but technically it is no problem to integrate it into the circuit switched or packet switched telephony system. But it should be user definable to subscribe itself to such a service.
19. No, In US, emergency broadcast are done via radio and television. A new system 'Amber Alert' is based on the highway-motorways that flashes the alert for kidnapped children.
20. Yes, Imagine that everone in the country/world who is faced with a similar situation is going to contact everybody via the phone! I think there are better ways to help such people, for instance dedicated programs on television.
21. No, Only if Caller-ID is visible (and right) and it's possible to block such calls. If calls are coming from an authorised office / department, I see no spamming behaviour. But such a case is built on different circumstances and you have to deal with it…
22. Yes/No, Even if this scenario is not according the definition in 2.1 I would say yes, but I would differentiate if it is done by the father/mother (yes) or done by the public authority like the police (no). In case it is a police VoIP emergency broadcast it could help to inform/warn people depending on e.g. location.or to gather information!
23. Yes
24. No, It should be regulated, and only autorized persons can broadcast call messages
25.
26. Yes, It would be "No" only if my end device offers a possibility to un-/subscribe to emergency broadcasts.
27. Yes, This could be abused..
28. Yes, Ich kann mit einem Anliegen jedwelcher Art ohne grossen Aufwand viele Leute erreichen, die in grosser Mehrzahl mit meinem Anliegen nicht betroffen sind. Auch wenn es für einen "guten Zweck" ist, ist es natürlich Spam.
29. No, Artikel 3 Buchstabe o des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG, SR 241) erklärt nur unaufgeforderte Massenwerbung für Waren, Werke und Leistungen als unlauter und damit illegal.
30. No, no commercial reason, desperateness
31. No, telephony emergency broadcasts are not VoIP Spam; however, if an attacker is able to exploit the emergency broadcast feature to use for his own means, then it becomes VoIP Spam. Technically, depending on the deployment of the emergency broadcast service, Sandvine can be configured to detect and mitigate and/or report that this action is occuring. Using a combinatoin of signature and behavioral-based techniques, Sandvine could detect the presence of the broadcast flag, or a system depositing into multiple accounts.
32. Yes, I do not believe that telephony is the appropriate channel to help recover lost people or lost objects. TV and radio is certainly more efficient, especially TV where a picture of the person/obejct can be broadcasted.
33. Yes, In solchen Situationen sollte besser die Polizei beigezogen werden
34. No, Not if performed by the operator (i.e from some kind of servers) towards users who previously agreed to be contacted in such a way for certain purposes (i.e emergency cases).

35. No, Generally this would be a community event/safety call and would not be considered Spam. However, if calls are made to every user at a business vs. just the main contact. the redundancy would have to be address.
36. No, couldn't see the relationship with your situation. Normally you have to sign up somewhere to receive emergency broadcasts - however I could emagine some (non-VoIP?) cases where all UEs in reach (where the network operator knows the physical location of the UEs, e.g. the DSLAM port# or antenna the UE is registered at) are warned of some situation (e.g. Tsunami warning). This I don't regard as unsolicited information
37. No
38. No, No, these are not of commercial nature. However, using speechtelephony as a medium does not seem very appropriate in these cases. Mass media such as radio and TV and messgages sent through SMS appear more appropriate.
39. Yes, Bei einer solchen Verwendung würde das Thema nicht mehr ernst genommen ("schon wieder jemand vermisst, ich mag gar nicht mehr hinhören..). Das Problem muss anders angegangen werden. Man sollte selbst entscheiden können ob ich SPAM lesen will oder nicht. Beim Telephon kann ich erst enscheiden, wenn ich das Telephon abnehme und höre.
40. Yes, I do understand the parents of a kid when they try everything. But the main point to classify something as Spam is the range of recipients of a certain message. If the parents broadcast a message to all their relatives and friends, this is something different than broadcasting their message for help to a million people.

A.1.3. Do you think you would use 'VoIP Spam' in such a situation?

***Situation**: Imagine that you are a father/mother of a 4 year old kid who is already lost for 2 weeks and you are getting desperate. You know a way to get a digital list of all telephone number in your region, how you could prepare your laptop to play a pre-recorded message on all these telephone number's mailbox in one hour and that 5000 CHF the maximum punishment is you can get for such an action.*

1. No, I think that there are better means, TV, Radio, Newspaper to broadcast such news
2. No
3. Yes
4. No
5. Yes, If desperate enough I might be tempted to use it - if the punishment is so low. However, I would know that it is wrong and counter-productive if many people do it.
6. No, Just it's SPAM
7. No, I think, that those actions -if helpful for the case- should be don by police forces
8. No, I say know, because I doubt it would help a lot if already TV stations and radion sent the emergency broadcast. I'd rather use the money to reward a person giving a hint that helps to find the kid. However, I've no kids and I don't know what I'd do if I'm very desperated.
9. No, very very odd. I'd talk to the police first
10. Yes, If you are desperate… If it's effective, it's another question…
11. Yes, Last hope to get my child back! I would do it.
12. No, ich denke nicht dass das in so einer Situation eine wertvolle Lösung ist.
13. Yes, Only if I saw that the police is not taking appropriate measures
14. Yes, siehe oben.
15. Yes, My daugther means everything to me.
16. Yes, I'm getting desperate.
17. Yes, see above
18. Yes, Of course I'm desperate.
19. Yes
20. No, I think it would not work. People will simply deny the message and react to it like they do react to 'classical' email SPAM.
21. Yes, Altough this is really SPAM (after the definition from BAKOM); I would do it! By the way: the fine from the current law is at CHF 100'000.--. BAKOM definition: Kennzeichnend für Spam ist vor allem die massenhafte, automatisierte Versendung. Sie macht es erst möglich, mit geringstem Zeit- und Geldaufwand viele Millionen Empfänger zu erreichen. Es kommt dabei nicht auf den Kommunikationskanal an. Ob E-Mail, Instant message, SMS, MMS, Fax oder Sprachnachricht: das Spamverbot gilt in allen Fällen
22. No, The public authority is responsible to help
23. Yes
24. No, We can have emergency operators - only these people can broadcase messages (answer is same as above). openness can easily be abused
25.
26. No, I would use the 5000 CHF to engage professional help.
27. Yes, This could be abused.
28. No, Klar, klingt verlockend.. ich frage mich dann nur, wie ich die Rückrufe managen könnte und vor allem wie ich die guten Feedbacks von den schlechten trennen könnte. -> ich glaube das wäre ein klarer Fall für die Polizei. Ob die dann SPAM als neue technische Fahndungsmethode anwenden könnte und so zu ihren Informationen kommt.. vielleicht? Da stellt sich dann aber die Frage, wenn ich so einen Anruf auf meiner comox hätte… wie stelle ich fest ob der echt ist und nicht bei einem Rückruf für mich hohe Kosten auftreten?
29. Das BAKOM kann zu dieser Frage keine Stellung nehmen.
30. Yes, well being of the child is worth more than 5000 CHF
31. Yes, This could be a valid public service and is not really VoIP Spam, similar to how Highway notice boards are used when a child goes missing. From a technical perspective, this type of attack would be similar to a botnet or other reconnisannce probing attacks that happen on the internet where a single device attempts to infect many devices. Sandvine's network integrity solution suite includes DoS and DDoS attack detection and mitigation, which can identify this type of behavior, independent of the actual

attack, and perform mitigating actions on this behavior, such as blocking or redirecting the attack, or creating notification and alerts of the attack.

32. No, In a desperate situation I would rather use the official channels via Police and media. In Switzerland there is from time to time a special broadcast just before the official news at 19:30 where the police asks for help from the public to recover a disappeared person. I would also search for a lost child first myself in the area where it got lost.
33. Yes, Hier wird eine Infolawine losgetreten, die von Einzelpersonen ausgehen kann ==> finde ich nicht vernünftig
34. No, The operator should offer this possibility (see 2.2). This must be anyway coordinated with the Regulator (Police) to centralize and validate any information coming back from such broadcast information. Doing this in a private manner would be anyway risky and not so efficient.
35. Yes, Spamming is relative to the recipient. If a user is interested or can act on the information, then they will not view it as SPAM. If a user does not care, cannot act, etc. , it will be viewed as SPAM. Also, if a user/family has multiple phone numbers, then the first one would be viewed as interesting and the other ones will be viewed as Spam. On the other hand, if value to the community is critical, it could be viewed as a value added service to the community whether the individual cares or not.
36. No, don't think it would help since people in that area are aware what happened anyhow (SPAM via radio/TV ;-)). I would leave it to the authorities to SPAM
37. Yes
38. No, No. See above for more appropriate means.
39. Yes, Es ist mein Kind…
40. Yes, If I am in such a situation by myself, then of course I would try everything. I would accept a punishment of CHF 5000.-. But this essentially means that either the punishment is too low to prevent people from doing this or we have to live with such 'spam' messages in the future. However, initiator of such 'spam' need to be aware that they are doing something illegal.

A.1.4. How easy do you think it is to Spam via Internet Telephony?

1. I would not know right now how to do it, but I am very sure, that I would find a "how to"-description on the internet I could easily apply and follow
2. in future tolls for anybody will be available
3. Nur für Experten
4. I don't know, but I can imagine that it could be easy
5. Not so easy that everyone can do it. But it is too easy to keep people with criminal energy away. There are toolkits for viruses, trojans and rootkits already. So there will be similar kits for SPIT attacks. SPAM is a business, SPIT will become one.
6. anybody can do it
7. I don't thin that you should be an expert, but I belive that more than 90% of PC users are not able to spam. (including me)I guess that one should be at least an advanced user of IT Systrems
8. Yes, but of course it needs some effort. Actually, accordung my personal definition, it can also be done with a normal TDM access, but it need more effort.
9. with technical knowledge pretty easy. E.g. for skype, there are countermeasures unless the chineese use their reengineered version to highjack Super Nodes, but there is also traffic mitigation. On the gateways, I think there is appropriate abuse protection.
10. Anybody with basic ICT knowledge. It is potentially easier to perform SPIT vs SPT (over normal telephony), because you may not need complex or expensive PSTN equipments (a VoIP Trunk will be cheaper than a PRI)
11. The INternet will provide us solutions, as usuall
12. Ich denke es ist recht einfach, mit einem PC an mehrere Peronen gleichzeitig Voice Messages zu senden, so wie man heute auch SMS SPAM generieren kann.
13. Spam is quite easy with open source SW like Asterisk.
14. SPAM ist nicht nur ein Internettelefonie Problem. heute gibt es bereits SPAM (vgl. Tele2 etc.); besonders ausgeprägt in den USA, wo es vom Regulator über "do not call lists" adressiert wurde. Auslöser für SPAM sind mE primär: Flat Rates/ Terminierungsprese von 0 und die Möglichkeit die eigene Identität zu verschleiern (dann werden nämlich die do not call lists wirkungslos)
15. Very easy as soon as free available tools allow simple scripting. As soon as more and cheaper AVR and TTS provider will enter the VoIP market, Voice Spam will increase.
16. Are the telephones numbers as a start traded directly and thus published, everybody can buy the accounts and can SPAM via internet telephony. A potential hacker required just once the right tool. Even it will be easier if a carrier use VoIP number range for his SIP customers. A potential SPIT'er can use this range and polling the list. http://www.bakom.admin.ch/themen/telekom/00479/00604/index.html?lang=de
17. It will be easy as long as the system is open or has weaknesses. We saw such spammings for Instant messaging systems like ICQ. Therefore, as long as there is a Telco or VoIP System somewhere that isn't protected enough, it will be easy for for experts to to spamming. I don't think that it will be easy for non-experts to do spamming, as these weak systems will be closed as soon as experts have already used them.
18. It is quite easy, not only for experts. Free open source traffic generators for the SIP protocol are already available. In comparisson with the email-threat you can even buy the "service" of spreadingmessages. The same will apply for the VoIP SPAM.
19. Difficult today. Maybe easier tomorrow with hackers tools availability
20. It is only possible for experts until one program (written by an expert) becomes publically available.
21. it's easy, you can download programs & usermanuals from the internet
22. SPIT can be done by anybody with access to Internet or ISDN/POTS
23. Ich denke das es auch möglich ist ohne ein Experte zu sein
24. It is easy, in a small scale even Vonage, AT&T callvantage etc can be spammed. However, bulk spam calls are difficult because still these companies operate in island manner.

25.
26. Technical it's easy, but service providers are responsible for the commercial possibilities (i.e. free calls)
27. Spamming is posible for experts or non experts that have been equipt with the appropriate tools.
28. In einer ersten Phase werden es wohl eher wenige wirklich effizient machen können, aber sicher schon bald wird es entsprechende Tools auf dem Internet geben, die man einfach benutzen kann. Je nach Firmenphilosphie des Service Providers, des Homenetworks und der Applikation (Security, Firewall, AAA, …) wird es dann auch mehr oder weniger gut möglich sein..
29. Das BAKOM geht davon aus, dass versierte PC-Nutzer die dazu notwendigen Programme im Internet finden können.
30. not so easy to do, however, it is probably easy to find somebody who knows how to do it
31. Sandvine has conducted some preliminary research on VoIP attacks. Successful DoS or DDoS type attacks on a VoIP service yield similar results as they do with any other type of service. DoS or DDoS attacks are easy to deploy and do not require much expertise. Our current assessment for most VoIP attacks (non-DoS or -DDoS, where the goal would be to successfully deliver a message) is that removing the 'man-in-the-middle' ability from the attacker makes attacks more difficult; however, like any attack, VoIP attacks will get easier over time. Better tools will be produced to permit the non-expert to launch attacks. Sandvine is actively working in this area of technology. For example, during our reasearch, Sandvine was successfully able to deploy a 'Ring Attack' on a set of clients. Some basic intelligence gathering was required before the attack. Successfully executing a 'BYE attack' was much more difficult.
32. I would not be able to do it without investing lots of time in studying ways of hacking account and learning how to use hacking software. You need lots of time to do this. I think you need to be quite a bit knowledgeable to in SIP and writing viruses in order to be able to do it.
33. Es ist eher einfach, je nach Möglichkeit, die Softclients bieten und je besser die Informationen im Internet sind..
34. Sending SPAM is always easy but more difficult is to send SPAM with a minimum of risks (from a legal point of view)… And this depends on the infrastructure used. In a free Internet environment it can be quite easy; in a "secured" environment like in IMS it will be a bit harder as you have to brake down encryption/authentication mechanism to eventually steal a user account (or you have to create a malware).
35. Initially this will be fairly difficult to do. Again, the authentication component of the device/softclient could be hidden from the user to make this difficult or impossible.However, once someone has done it once, then that technique/software could easily be shaed across the spamming community so others can take advantage of it. Once this starts, it might be difficult to stop. In fact, introducing techniques that limit the number of calls a user can place over a period of time might be a good mechanism to stop this.
36. professionals could do it, needs some programming knowledge to set-up call lists and play pre-recorded texts
37. Ich bin der Ansicht, dass es für "effektivern" SPAM welcher dann auch grösseren Schaden anrichten kann, ein umfassendes Wissen (IP Technologie, Hardwarespezifikationen, Software-Entwicklung, etc.) braucht. Dieses Wissen ist an Hochschulen, Berufsaubildung wie Informatiker oder Hackerkreisen lernbar.
38. Depends on the implementation of the protocols in use. Especially inmportant are authorization mechanisms.
39. Kommt auf das jeweilige Anti-Spam-System drauf an. Aber Grundsätzlich ist Spam über VoIP ganz einfach - Tools sind für jederman verfügbar
40. There will be/is software available which will make it very easy. However I think that the problem will only become a real problem when phone calls are as cheap as e-mails.

A.1.5. What do you think are the most successful methods for Spamming?

1. see 2.4. I do not know yet, but Robert and Mark will tell me
2. unknown
3. Keine Ahnung
4. I can imagine sending spam e-mails to a text-to-speech engine
5. The same methods as used for Spam: Trojans turn a great number of computers into zombies which make a small number of calls each. The zombies can be rented and fed according to the needs of whoever wants to sell something.
6.
7. I have no idea
8. Zombie network
9. P2P-Bots
10. Neither nor. Your own infrastructure, because you need a ITSP (Internet Telephony Service Provider) to route your calls to the PSTN, where your targets are connected. You don't care to anonymise yourself, as telecommunication law ensures that: 1) you can place calls 2) there's no limit on the volume of calls you want to place, as long as you pay for it 3) the operators cannot eavesdrop on your communications. You don't want to let your credentials circulating in your own malware, potentially discovered by reverse engineering. With Caller ID suppression, you avoid direct complain from the targets. Until one decides to start a procedure with the operator, you have already placed your thousands accounts.
11. Mass SPAM-Calls
12. N/A kenne mich zu wenig aus
13. Don't know
14. weiss ich nicht
15. Anonymous AVR and TTS provider.
16. With spambots (a robot that combs web sites for phone numbers, a bot contained inside a Trojan that compromises a computer, a program designed to shield an ISP) you can collect on a very easy way the VoIP addresses from the internet. Another very effective way is, to hack in to a database (e.g. ENUM) to absorb unauthorised the corresponding information.
17. EMail: Zombie networks (they base partially on trojans?)
18. bot-nets, which attack the VoIP community with SPIT (SPAM over Internet Telephony)

19. Zombie network
20. A Zombie Network.
21. Zombie Networks; Botnets ???
22. installed freeware/Opensource tools/software like sipp, sip bomber, sipper, sipness, asterisk, ser etc.
23. Kann ich nicht beurteilen
24. These methods are more futuristic….right now simple logic of spitting can be used from a single or a small set of machines. Later on, spammers will opt for stealthy attacks…the methods you mentioned.
25.
26. Over 80% of SPAM today originates from SPAM zombies, i.e. infected hosts. Exactly the same tendency can be expected with SPIT, since it is relatively trivial to make an infected endpoint send large volumes of INVITE or SUBSCRIBE requests, send messages upon answer etc. The adoption of VoIP SPAM will be highly dependent on the commercial gains that can be achieved through advertising messages or VoIP phishing.
27. No idea.
28. Es wird wohl die Kombination von allem am sichersten und schnellsten zum Erfolg führen. Social Engineering (für Passworte, …) ist wohl auch nicht zu unterschätzen. Hier ist es auch wenig aussichtsreich, ausschliesslich mit technischen Lösungen zu arbeiten, weil die "Schwachstelle" ein Mensch ist.
29. Das BAKOM hat hier keine Präferenzen. Die Antwort auf diese Frage hängt vom Stand der technischen Abwehrmechanismen ab.
30. no idea
31. Sandvine Security Operations has seen that presently most spam is connected to botNets. In many cases these are small botnets of computers that are being controlled by an external party. Owners of these systems are typically not aware that they are spamming or are a participant in a BotNet. Security Operations has done some investigations into Onion Routing (the Tor network being the most popular). Executing an attack such as the distribution of Spam through this type of network is possible and has been detected by Sandvine. However, today there is usually a requirement to send large amounts of Spam in a timely manner in order to make it worth while. Using Tor and other similar networks for this purpose is not very productive due to the slow nature of these networks. BotNets used for Spamming ideally want Zombie devices that are on fast networks, as spread out as possible, and unencumbered by behavioural detection technology.
32. I guess that there are some robots which scan the entire Internet for e-mail addresses. These e-mail address lists are then sold to spammers who can use them to run spam on behalf of companies financing this kind of doubtful business.
33.
34. Based on the answer provided in 2.4 : it depends also on the type of network used. I am not that familiar with any Spamming "how-to ?" but I would say that for me creating a Trojan that would be propagated over E-mail for instance and would then create VoIP calls to the sip contacts in an address book would be quite efficient.
35. No opinion on this
36. trojans to create zombies etc. May however not work for SPIT so easily
37. Anonymisierungstechnik im Internet. Der IP-Traffic wird über eine Adresse die ganz leicht von der effektiven Adresse abweicht über mehrere Router weitergeleitet, so dass letztendlich nicht mehr ersichtlich ist, wohin der Traffic effektiv geleitet wird. Der User hat so keine Möglichkeit zu erkennen, dass was nicht stimmt.
38. Zombie (botnet) networks.
39. ? Ich bin kein Spammer….
40. It depends on what you want to do, if it is human-initiated phone calls there need to be front-robots which try to call somebody until the callee picks up the phone. then they get connected with the human operator. If it's robot-messages I think that renting a zombie network could be quite useful.

A.1.6. How is the current situation concerning VoIP Spam?

1. I am using VoIP since three month (BluewinPhone) and have no complaint so far
2. in Europe still ok
3. Weiss ich nicht. Ich hasse Vertreteranrufe, die einem irgend etwas verkaufen wollen oder irgend welche Umfragen über irgend einen Blödsinn machen. Das ist bei mir in den letzten 3 Jahren etwa 20 Mal vorgekommen. Mit Reklame Meldungen von einer Maschine wurden wir noch nie gespamt..
4. No idea
5. Don't know. I suppose it exists, but I do not have figures or personal experience. I expect that the problem is small currently because the community of VOIP users (in CH) is small. With the growing of the community SPIT will become attractive.
6. 1 - 3 calls per day in Europe, up to 10 in the US
7. No idea, but I guess it is not very critical for the time beeing
8. Seldom I get calls from e.g. marketing survey companies
9. not heard anything yet
10. It's already there, Combox Spam, SMS spam, Telemarketing, short calls (or just ring calls) to incite guilible customers to call back.
11.
12. Bisher bei mir nicht bekannt, ich benutze Bluewin Phone und Skype und habe noch nie Spam bekommen
13. I don't think it is critical yet. Everybody sees it as a massive threat because of the low costs to distribute it (similar to e-mail). Hence, it will become critical and widespread as soon as more people are frequent VoIP users.
14. SPAm ist nichtr nur ein VoIP Problem. Im Moment ist es de facto noch kein Problem . Die einzige heute verbreitete VoIP methode Skype ist gerade nicht so SPAM anfällig, weil man typischer weise nur mit Kontakten telefoniert und der PC in der NAcht ausgestellt ist.
15. A sleeping danger.

16. IP telephony is not widely used. So today, SPIT is not much of a problem yet. But it will become increasingly common over the next several years. There is a last respite as is generally known that the first attack will taking place outside from Switzerland
17. It did never happen to me and I'm not aware that we had such situations on our system. As long as VoIP networks are operated "carrier grade"or calls are billed, we will not encounter a critical situation..
18. There is already some VoIP spam observable, less than in traditional circuit switched telephony but NEC found an increasing hints of accidents in the internet. i.e. see http://article.gmane.org/gmane.comp.voip.security.voipsa/1336
19. Not much
20. I have no idea
21. VoIP spam is an as-yet non-existent problem; we are dealing still with Voice-spam.
22. As a permanent VoIP user with several public numbers I have never encountered VoIP Spam to my private CPEs.
23. Zumindest in der Schweiz hört man selten von Problemen
24. Spammers are waiting for critical mass of subscribers and overcome the PSTN.
25.
26. A few incidents have been reported in Japan. It is expected, that it will increase, but not reach a level like email spam.
27. At the moment there is only limited spamming but this will increase when VoIP adaption rate grows.
28. Ich habe bei einigen Demos gesehen, was möglich ist (alle Telehpone klingeln lassen, auf jemanden anderen Kosten telephonieren, …) aber diese sind wohl noch Einzelfälle. Heute zumindest noch..
29. Das Problem ist real. Zwar gibt es z. Z. weit weniger SPIT als SPAM. Die Beeinträchtigung der Empfänger ist aber bei einem SPIT-Anruf wesentlich grösser als beim Erhalt einer SPAM-E-Mail.
30. no big problem yet
31. Currently Sandvine feels that VoIP Spam is in the early stages of software development. We have seen indications of some 'initial testing' and have performed some analysis on some 'proof of concept' software that has been released on the Internet. We expect VoIP Spam to increase as more businesses and individuals obtain VoIP either as an additional service or replacement to their current POTS lines.
32. We currently get calls from call centers with real call agents (people); so far we do not get automated machine-generated Spam calls.
33. Zur Zeit ist SPAM aus meiner Sicht kein Problem
34. Currently I do not have any other information than the one available in the Internet; some case in America, more in Japan.
35. We are not aware of Sylantro customers encountering Spamming.
36.
37. --
38. OPTA has not received a single complaint despite massive uptake of Internet (IP) Telephony in the Netherlands.
39. VoIP ist noch nicht sehr etabliert bei Telecom Firmen.. Von daher eher neu
40. In my opinion at the moment it is just a catchphrase. For certain networks like skype the problem of voip spam is mainly solved by using a strong whitelist approach. I am using a VoIP phone from sipcall.ch at home and never ever received spam calls. I think in this case it's also because my phone is not recognizable as a voip phone. I'm quite sure, however, that voip spam will become a problem when there are 'real' flat rates also between different operator networks

A.1.7. Do you have one or more (real) examples of VoIP Spam?

1. no
2. no
3. Siehe 2.6
4. No
5. no.
6. Klassenlotterie from Germany or Financial services
7. no
8. see above: of course this does not meet the "bulk" criteria to be spam.
9. nope
10. cf 2.6
11. no
12. nein
13. No, I don't have an example
14.
15. No
16. SPIT incidents are already being reported in Japan (http://www.voipsa.org/pipermail/voipsec_voipsa.org/2006-March/001326.html) - Many computers are already infected and ready to be used for SPAM or other purposes including SPIT.
17. …no, perhaps unwanted contact subscriptions in Skype or ICQ?
18. lottery, adult websites, advertising, phishing
19. No
20. No
21. we have different, ongoing examples from the TDM world! E.g. callee gets calls from Italy during the whole day… Note: the problem is always concerning the callee: what is his personal attitude towards SPAM? where is his threshold of "pain"?
22. No
23. Nein
24. any approach which can setup a session
25.
26. http://voipforenterprise.tmcnet.com/feature/service-solutions/articles/4009-spit-bringing-spam-your-voicemail-box.htm
27. No. I have never expirenced it personally.

28. ich habe bis jetzt keine konkreten Fälle, die ich bemerkt hätte.
    -Werbeanrufe genereller Art (die letzten aus Italien), die mit VoIP und Flatrate immer wie günstiger werden.
    -Aber bisher wurde mein Bluewin Phone noch nicht geknackt und es läutete einfach so.
29. Die bei uns eintreffenden Klagen betreffen meistens Aufforderungen, über eine gebührenpflichtige Nummer (090x..) an einem Gewinnspiel teilzunehmen.
30. advertisements via fax are growing dramatically. Selling of 'Deutsche Klassenlotterie' is also increasing massively
31. Sandvine has tested a few VoIP attacks. One attack was used to quickly send INVITE and then BYE messages to a target in an attempt to cause it to fail. Another attack was used to send INVITE messages with obfusicated fields in the SIP packet. Another reconnissance attack used the OPTION command to gain information on a target prior to attacking it.
32. There seems to be a trade of phone numbers when you purchase some products and put your phone number down (e.g. customer membership in a shop). E.g. say you want to lose weight and you register for a wait loss program in one of the well known programs. Then you may receive phone calls from special beauty clinics or other weight loss programs, because your phone number has been traded among these organisations.
33. A second example is from the business environment. Usually when attending conferences, you have to provide your contact details. This is gold value to the organisations selling conferences. I have been spammed several times for conferences. But again, this is done by real humans in specialised call centers. I have used to receive up to 10 call attempts per day (number hidden). Typically Marcus Evans are specialising in this type of campaigns.
34. keine
35. No.
36. No
37. I received (TDM) calls (2x) with spoofed calling party numbers (inexistent international country code) where I believe that the source was VoIP ("congratulations, you have just won a cruise in the caribean. To collect your price press 9…")
38. --
39. No
40. Nein, nicht betroffen
41. No

A.1.8. Do you think VoIP Spam will be a problem in the future?

1. Yes, It is like email and Spam and unfortunately it will follow the same way
2. Yes, flat rate offers from operators
3. No, Ja nur, wenn Flatrate ohne irgend welche Limiten kommt
4. Yes, IIf there are possibilities, many people will use them
5. Yes, VOIP will become a boom with flat or zero rates. When the community is large enough SPIT will be successful just like Spam.
6. Yes, Because we will have flat rate for voice calls
7. Yes, I see is a enormous potential for comercial/industrial applications and therefore I belive spam will be viewed as a problem
8. Yes, - it's easy to do; - it's already done by e-mail; - it's more effectly than e-maill because people need longer to listen and recognize it as spam; Perhaps, we can avoid it, if we still charge termination of calls?
9. Yes, ithere is no reason why it shouldn't. There is a pontential to harm and a potential to earn money, if voip broad or multicasts calls are for free.
10. Yes, Same as today: I don't see a difference between VoIP and classical Telephony. Maybe it is easier with VoIP, if ITSP provide large VoIP trunk to a cheaper price than TDM trunks. Same is about the price of a single call. Telephony SPAM will evolve accordingly to the cost of Phone calls and infrastructure, not to the type of underlying technology. Consider the business case of the spammer. Email Spam is extremely popular because you can send millions of emails for almost nothing (couple of cents). Phone calls are currently much more expensive.
11. Yes
12. Yes, Es wird sicher Leute / Firmen geben, die diese Möglichkeit ausnutzen.
13. Yes, See 2.6
14. Yes, Siehe oben: Flat rate/ keine Terminiierung, einfach, immer neue identitäten anzunehmen.
15. Yes, Spam is hard to fight and even harder to beat. TTS and AVR systems getting better and more sophisticated every day.
16. Not if we well known our customers and have a very restrict interconnection and peering policy (Only with carriers and providers they known theirs customers as well). Of course, VoIP services will be almost free and there is opportunity for illegal and aggressive telemarketing. But if we locate a SPIT'er by using filters and upper limit on initiated calls, we have the possibility to prevent SPIT.
17. Yes, Given the business that EMail Spam creates today, it will be a matter of time when it swaps over to VoIP
18. Yes, It seems that VoIP develops similarly as email, that means that most VoIP call will be spam calls in the future. VoIP spam calls will cost nearly nothing for the spammer in contrast to CS calls.
19. Yes, Yes but is no different than todays computer based calls with machine voice.
20. Yes, Just like with email, spammers wil try to use this medium.
21. Yes, technology is changingg and so the behaviour of the spammer
22. Yes, More people will use VoIP and will quickly recognize that it is easy and cheap to advertize for something or make surveys with e.g. Robots or Agents.
23. No, Ich denke das wir unsere Netze genügend schützen können
24. Yes, Any communication medium that can be used for making money will be abused
25.
26. Yes, Absolutely - we can anticipate very similar trends to Email SPAM today. Some SPAM attacks may be used as DoS attacks to overwhelm SP infrastructure, voicemail servers etc., but the majority is likely to be for commercial gain through advertising,

phishing etc. However until we have broad-adoption of SIP trunking and IP PBXs accepting calls from any other SIP device on the network, the scope for VoIP SPAM is limited today.
27. Yes, Spamming will increase when more users switch to VoIP.
28. Yes, Wenn wir und als Provider nicht genügend gut darauf vorbereiten, könnte dies sehr wohl zu einem Problem führen und zumindest unsere zahlenden Kunden verärgern. Als (undenkbarer) worst case könnten sogar Businessmodelle ausgehebelt werden, -> Warum bezahlen wenn es mit einem Trick (Download vom Internet…) einfach gratis geht?..
29. Yes, Die Telefonkosten sinken stetig. Zudem gibt es immer mehr Teilnehmer, die gratis via VoIP erreichbar sind. Damit sinken auch für SPIT die Kosten gegen Null, was Voraussetzung für breit angelegtes Spamming ist.
30. Yes, if it is cheap and easy to produce yes
31. Yes, Sandvine believes VoIP Spam will follow a similar pattern as e-mail Spam. As more and more consumers turn to VoIP services to replace their land lines, as more and more answering services are deployed, and as more and more PDAs with answering/messaging services are deployed, the VoIP consumer base grows large. Just as e-mail Spam has increased as more and more people and companies have started communication via e-mail and the Internet, VoIP Spam will gradualy increase.
32. No, because we will make sure that Swisscom customer's data will be safely guarded and we will have the proper preventive counter-measures. Consequently it will be very hard to hack an account from which calls can be made.
33. Yes, Je mehr Personen VoIP nutzen, desto mehr muss auch mit SPAM gerechnet werden.
34. Yes, This will be surely a subject of discussion but the real impact on IMS networks is hardly predictable.
35. Yes, As VoIP becomes prevalent, the ability to create calls with just PCs will become more pervasive vs. the old world where CTI equipment was required. The other Spaming option is use of the Click to Call function that may introduce abusive behaviors.
36. Yes, flat rate tarifs, uncontrollable internet with (flat rate?) gateways to "controlled" VoIP areas
37. Yes, Die geniale Technologie VoIP wird immer breiter eingesetzt. Die Aufwendungen die SPAM zu vermeiden wird immer aufwändiger, was letztendlich zu immer höheren Betriebskosten führt. Dies wiederum kann dazuführen, dass die VoIP Technologie an "agilität" und "performance" verliert und somit in der Anwendung für einen grossen Teil von Anwendern uninterressant wird.
38. No, It appears operators currently use enough security measures to prevent it or it has not reached the mass to make it interesting yet.
39. Yes, Gleich wie E-Mail
40. Yes, It all depends on the price of voip phone calls and the price arrangements between different operators. As long as there are still barriers (speaking of price) between different operators, voip spam will be few. But in the future, phone calls will be free (a.k.a. flat rate) worldwide, which definitely will be a problem.

A.1.9. How effective do you think technical countermeasures can be?

1. comparable to email Spam filter. It will always be a tradeoff of total restriction and total openness
2. good
3. Schwer abschätzbar. Dazu müsste man erst typische Parameter, Verhaltensweisen von Spamern erfassen, qualifizieren, quantifizieren.
4. They are surely effective, but I think they wont be enough.
5. a) not very effective if the voice service should be convenient like the conventional phone service. b) very effective but also very likely to produce false positives when strict counter measures are implemented. Furthermore, strict counter measures will mean very limited usability of the service.
6. mid
7. I am pretty confident that technical measures will help a lot
8. Even if they are very effective; I don't believe they will be good enough and there will be always a uncertainty where people have to check if it is spam or not (exerience with e-mail) And the defence expenditure will be high, I guess.
9. very effective, but the best is to provide legal countermeasures and destroy the business plan for spam
10. could be, but major impact in the simplicity of use of the actual phone system. Again, SPIT will be an issue if calls are free or extremely cheap or easy to fraud. It’s mostly a provider issue: if the provider authenticate correctly its users, if calls are not free, and if he can deter effectively fraudsters (subscription fraud will be an issue), then SPIT will be contained. If one of these conditions is broken, then we end up with Spam, and over all networks
11.
12. Wie beim Mail wird es schwierig sein, Spam immer zu erkennen und zu blocken.
13. It's always a trade off between costs, effectiveness and useability. The more effective a countermeasure is, the more it costs (normally) and the less user-friendly is the service.
14. Das problem dürfte technisch kaum zu lösen sein (vgl. E Mail), sondern muss zusätzlich auch kommerziell angegangen werden (z.B. über das zukünftige Interconnection Business Modell)
15. Have a look at SMTP based spam and you can easily answer the question yourself.
16. Technical counter are not very effective and quit hard to hold it up to date. Furthermore all this lists and counters are not very comfortable for our customers and ourselves (busy by the first attempt, challenge the caller and announce alternate reachability). These preventive measures imply most human action before calling and cause a bad impact on the user experience. Besides, a SPIT'er will use only once an account for an attack.
17. It will not be possible to avoid this - SMTP proved it every day. But I hope that the measures we have today to avoid abuse in PSTN networks with data mining CDRs will help here too.
18. Similar to email spam protection. The protection system must be frequently updated with new threat definitions.
19. Legislation and technology. End user phone has caller id blocking mechanism.
20. Very effective, probably comparable to SPAM filters for email.
21. In some cases it's not preventive; huge complexity. Problems also with calls from other countries: correct Caller-ID? .

22. depending on the implementation it could measure a huge amount of observations but it may need a lot of computation power (on demand calculation or based on billing information, huge database). It might be necessary that the database has already values included before the calculation can start..
23. Kann ich nicht beurteilen
24. Still, there is no effective counter measure
25.
26. Some of the basic mechanisms under discussion today e.g. blacklists, whitelists etc. may not be very effective, since IP address spoofing and caller ID spoofing are relatively trivial and tools are widely available today. Gray listing is a risky mechanism, since the history of Email SPAM shows that the majority of SPAM comes from infected endpoints. If a VoIP endpoint is infected and starts spamming other hosts on the same network, it is possible for an attacker to execute a very effective DoS attack on an Enterprise voice network as all infected VoIP endpoints are graylisted due to "bad behavior". This could bring large portions of an enterprise voice network to a standstill. Gray listing can only be deployed when there is a very low chance of false positives, and endpoints are protected with AV, host IPS and patch management solutions. Content analysis could also pose a problem, particularly on real-time traffic, since analysis introduces a time delay and is ineffective on encrypted traffic. The most effective mechanisms are likely to be those that focus on statistical and pattern analysis combined with reputation-based mechanisms to identify suspicious endpoints. Similar to spamming today, SPIT zombies would be likely to establish contact with botnet command and control servers, send large volumes of SIP INVITE messages etc. A reputation-based system would rank the integrity of an endpoint based on contact with suspicious servers, callee feedback, belonging to a non-trusted domain etc. The above mechanisms can help identify a spammer and block calls from a suspicious endpoint. This could be combined with whitelisting to avoid the dangers of false positives.
27. I do not have any experience in this fiield but I do imagine that appropriate measures can be put into place.
28. Technische Hürden können vielleicht gewisse Muster erkennen (Massenrufe, …) und Manipulationen erkennen, aber das dürfte ziemlich schwierig werden und eher auf klare Fälle ¨hinweisen. Wirklich effizient ist, wenn man die Systemlösungen von Beginn weg entsprechend designt (Security, DMZ, ..) und dafür die entsprechenden Konzepte zuvor erarbeitet und auch austestet. Dies bedingt naürlich gutes und vor allem aktuelles Know-How und entsprechende Desingrules / Anforderungen für die Systeme / Supplier. Technisch gesehen sollten gut designte Systeme alles bis "heute" bekannt ist abfangen können. Dies bedingt natürlich ein permanentes review und update der Systeme gemäss den neusten Erkenntnisse aus den einschlägigen Sites.
29. Das BAKOM geht davon aus, dass technische Filtermassnahmen wirksam sein können. Wie bei den E-Mails wird es aber nicht gelingen, SPIT zu 100% auszufiltern. Zudem beeinträchtigen zu scharfe Filter in der Regel auch die vom Empfänger gewünschte Kommunikation. Das Abwägen der Wirksamkeit der einzelnen Massnahmen gegeneinander ist nur bedingt möglich, weil die Spammer ihre Methoden jeweils ändern, wenn eine Filtermethode verbreitet angewandt wird.
30. > 80%
31. Technical counter measures (assuming defensive measures only) are quite effective if deployed properly. Sandvine believes that behavioural detection and mitigation is the best way to deploy counter measures. Sandvine has been researching, detecting, and blocking attacks since its inception. VoIP is another application that has some similar and some new attack vectors. By deploying Sandvine's network integrity solution suite, these detections are successful across attack vectors, regardless of the attack tools and signatures used.
32. I think this is where our attention must focus initially. What we need are mechanisms where we detect that someone is making a large number of calls which is not normal for a classic residential. If a residential exceeds this limit, it raises an alarm in the NOC. Also, as a residential, I want to be able to say that I do not want to receive national calls without caller ID. Most of call centers hide the caller ID. I think there are some basic mechanisms which can be put in place to make it a bit harder to spam. Another way would be to limit the call rate: you can make 100 calls back to back within a period of time but then on you have to wait 1 minute before you can make the next ones..
33. Grundsätzlich bin ich der Meinung, dass mit solchen Möglichkeiten SPAM reduziert werden kann. Ich denke, dass nicht alle gleich effizient sind, dass man aber möglichst viele Möglichkeiten zur Verfügung hat, damit in der Praxis je nach Problemart dann entsprechend vorgehen kann. ==> Die Bekämpfung wird sich wie die Cration von SPAM-Möglichkeiten ensprechend entwickeln.
34. Measures like Black/White/Greylisting are surely efficient but would not help in the case where the subscriber was infected by a malware. In order to protect the core nodes from overload in case of massive attack we could speak about Call gapping and Admission control.
35. Like any security issue, there will need to be iterative development to close holes and traceability of the offenders. Initially, metrics are critical as well as customer complaints (and proactively soliticiting those complaints. Note that SPAM from the PSTN or VoIP are not detectable from an end user.
36. 80%?
37. Sehr effektiv, wenn die Kunden bereit sind die Kosten zu bezahlen!
38. Very. Will depend greatly on inter-network authentication and implementation of strong user authentication schemes.
39. Wenn gut implementiert --> GUT
40. they can be very effective, but in contrary to e-mail, content analysis will be almost impossible, especially if you want to prevent voip spam before ringing.

A.1.10. How effective do you think legal countermeasures can be?

1. I think the legal measures belong to our system, though the effectiveness will be small, due to globalization
2. ok
3. Sehr wirksam. 10 Jahre Gefängnis hat niemand gern :-)
4. They wont be very effective. I there is any profit for any country, it will never accept to collaborate
5. Necessary but not very effective (just like the situation with Spam). An attacker might simply go to a country with not so strict legal counter measures and no agreements regarding punishment of SPIT.
6. mid

7. Will only help a little bit if the spamer is local. In most cases the source will be somewere in the world.
8. They only work within a trusted network, where it is not possible to spam anonymously
9. pretty efficient if it comes to usa
10. is a pre-condition to the other measures, especially the ones initiated by the operator. Analogy: computer dialers to dial-up to 0900 numbers: only once Bakom ruled this was illegal could we intervene rapidly and on behalf of the customers.
11. inside Switzerland we have a chance to act against SPAMERS, but they are clever and they act from foreign countries.
12. Auch hier wird es nicht möglich sein, gegen alle Missbräuche vorzugehen.
13. They can have a deterrent effect and keep number of spammers lower than without legal counter measures
14. Tragen dazu bei ; Weil aber Identotäten immer unklarer werden (Anonymität) idürfte der Wirkungsgrad beschränkt sein.
15. see above and ask China, Russia and those kind of countries.
16. At this stage, it doesn't work today for SPAM ;-)
17. It will avoid attacks in countries where these laws will be applied. But if an attacker is in a country where no legal prosecution is done or when an attacker can hide its origin, legal measures will not help
18. Legal counter measure could be helpful, but only with limited effectivness. Legal loopholes will be found out or other methods will be found how to bypass the law. In the CS telephony system we have stil spam calls for advertisement although this is forbidden by law.
19. Somewhat.
20. Hardly effective because legal countermeasured are restricted to just some countries. SPAMMERS can thus move to countries were the legal counter measures are not present or less restrictive.
21. SPAM originates mostly from mistrusted countries; so it's hard to catch the spammer. Counter measures inside Switzerland are in place; fine up to CHF 100'000.--
22. Sounds like a good solution, may be a mix of A1, A2, A3, A4 would be the best. In example an addaptiv solution (cheap, quick and testable), which fits to almost every situation!
23. Eventuell als Vorgaben für Netzbereiber die ihre Netze zu schützen müssen. Eher als effektiv
24. Not effective, think of openness of Internet and its associated vulnerabilities
25.
26. The current situation with SPAM shows that legislation is largely ineffective. Some countries, e.g. Canada, have managed to deal with SPAM zombies by blocking offnet SMTP traffic by enforcing all service providers to comply, but this does not address inbound SPAM coming in from other countries/networks. Legal counter measures could certainly limit commercial SPAM, but would not influence the use of SPAM zombies for illegal means.
27.
28. Legal greift in vernüftiger Zeit wohl nur national, international unter "zivilisierten" Staaten wohl auch noch, auch wenn es länger dauert, aber mit bestimmten Staaten sind solche Absicherungen wohl nicht realisitsch / durchsetzbar.
29. Gestzliche Bestimmungen sind insbesondere dann wirksam, wenn der Spammer und der Nutznieser des SPAM in der Schweiz sind. Gegen ausländische Spammer hingegen sind auf dem Rechtweg oft zu viele Hürden zu überwinden.
30. probably not effective on a global base. However, within a country it can help. Punishment must be high, and it must be 'easy' for the offended to get a case started..
31. Legal measures can be expensive, difficult and very time consuming. Although legal measures or the threat of legal measures can be successful on a given individual or targetted company, there are usually requirements prior to taking legal action. For one thing, you have to know who you are taking legal action against. Many of the botNets and botmasters today are very good at keeping their identity secret and they are dilligent at this. Consequently, time and resources are required to discover them, and often this does not work. If you happen to discover the owner or company responsible, you require evidence in order to legally engage them. You often have to be able to prove that the evidence did actually come from them and was not spoofed by a different organziation. Again, this takes time and resources. Finally, internationally there can be issues with differing laws in different countries, and the costs to legally engage someone in another country can be high.
32. All this requires traceability. A customer must be able to chosse to receive ad calls or not to receive them. If a customer receives ad calls, he must be able to complain officially to the phone company, and should be able to lodge a complaint with the regulator which should fine the offending party. Technically, we need mechanisms which enable the traceability and maybe also the identification of a call as being an add calll. This works reasonably well with plain mail and stickers you put on the mailboxes, therefore we have to think of something similar for phone calls.
33. Wäre sicher eine gute Voraussetzung, um SPAM zu reduzieren/verhindern
34. In networks were the subscriber must be authenticated it might be effective; in others not really.
35. No doubt that legal implications will help, unless the Spamming comes form another country.
36. 0%
37. Die Gesetzgebung und die Umsetzung sind viel zu schwerfällig. Zudem wird die Umsetzung nicht in allen Ländern gleich gehandhabt. Und die IP-Technologie keine Landesgrenzen kennt werden die SPAM Initiatoren in Länder mit schwacher Umsetzung der Gesetzgebung ausweichen.
38. Very. Success will depend on the punishment.
39. GUT
40. If there were worldwide standards for punishment and especially enforcement, this could be effective. However, I do think that there will never be such a situation :-)

A.1.11. How effective do you think social countermeasures can be?

1. They should be backup by legal measures. The effectivenes will help prevent onetime spammer, but not professionals
2. not very effective
3. So im Sinn: Kids weg vom Computer und raus auf den Fussballplatz? Wohl wenig wirksam. Etwas verrücktes anzustellen ohne dafür bestraft zu werden ist immer interessant für die Coputerkids.
4. I don't believe in that kind of counter measure.

5. Not effective at all. There will always be people who answer these calls or buy things. Just like spam. Although there are very few people who do reply it is still a business. The operator based process will be too expensive in the operation.
6. low
7. I don't think this will help much.
8.
9. very effective if you manage to outlaw spamming in a society right from child birth.
10. ineffective, as long as no legal background is present. Huge technical difficulties in identifying the originating network (too many interconnections, multi hop, no traceback capabilities).
11. This can be effective for a certain percentage of the SPAMERS. But a lot of them don't care and l continue as long they earn money.
12. Diese werden bei "Verbrecher" kaum wirken.
13. Probably not so effective to keep the number of spammers low, but effective to create awareness on how to deal with it
14. glaube ich nich daran (iSwisscom ist nicht die Instanz, die das Verhalten ihrer kunden zu überwachen hat)
15. see above
16. Criminal power could not be controvert by social counters.
17. does it work for EMail spam today? No.
18. They could help in mitigating the problem
19. Depends on many factors - penalty, availability of other means of communication - contacting local radio, television, emails etc.
20. Not effective
21. effective for local Swiss-user; ineffective for other countries.
22. Sounds like a good solution, may be a mix of A1, A2, A3, A4 would be the best. In example an addaptiv solution (cheap, quick and testable), which fits to almost every situation!
23. Niicht effektiv man sieht das ja heute beim E-Mail SPAM
24. it can be effective, but how to build it. trusting a competitor is difficult, what about "bad mouth attacks"…..
25.
26. Not effective at all, since finding the originator will be nearly impossible with spoofing and highly distributed attacks from infected hosts.
27.
28. Wenn man das Problem in den Griff bekämmt hätte man meiner Meinung nach mindestens die Hälfte des Jobs (Aus Risiko - Sicht) gemacht .
29. Immediately Contact Originator: Hier kommt die schärfere Massnahme gemäss Artkile 83 Absatz 3 der Verordnung über Fernmeldedienste (FDV, SR 784.101.1) zum Zug: Hat eine Anbieterin Kenntnis davon, dass eine ihrer Kundinnen oder einer ihrer Kunden über ihr Fernmeldenetz unlautere Massenwerbung versendet oder weiterleitet, so muss sie umgehend den Versand dieser Nachrichten sperren bzw. den Aufbau der entsprechenden Verbindungen verhindern. Sie darf Kundinnen und Kunden,welche unlautere Massenwerbung versenden oder weiterleiten, vom Fernmeldenetztrennen. Do Not React: Wenig wirksam. Da SPAM fast gratis weit gestreut werden kann, ist es für Spammer auch dann rentabel, wenn nur jeder Tausendste das Angebot annimmt.
30.
31. Social counter measures are not very effective. Social counter measures have been ineffective on Spam, and Sandvine expects VoIP Spam to be the same. Like e-mail currently, VoIP will become an easy way to access a very large customer base. The cost of advertising over VoIp will be very low.
32. Indeed you need to have the technical enablers to implement the operator reaction. I think you cannot have the one or the other. Both of them must be implemented to enable successful mitigation of unwanted spam calls. Traceability plus monitoring call levels is the key..
33. Eher nicht so effektiv ==> Bei Servern/Computer die SPAM verursache wäre dies vermutlich weniger möglich
34. Not so much otherwise we would have been successful already today for E-mail spamming.
35. A casual Spammer will react to this. A professional spammer will not be impacted and can move regularly to avoid detection.
36. 10%
37. Dies ist ebenfalls eine sehr effektive Massnahme um die Einengung von VoIP SPAM erwirken zu können. Letztendlich ist der Mensch entscheidend in der Bedienung von PC, Laptop, etc. !
38. Relatively Inefficient. E-mail spammers have shown they can hide their identity so easily that it is impossible to contact them directly. Negative rections do not deter if the profit remains high.
39. Weniger --> Anonymität
40. No way, enforcement will not be done -> see e-mail.

A.1.12. How effective do you think commercial countermeasures can be?

1. Interesting approach, which will prevent onetime spammers, but not professionals as these methods are probably not bullet proof
2. good
3. Sehr wirksam. Wenn der 501. Anruf Fr. 10.- pro Anruf kostet, macht niemand mehr Spam!
4. This could be the most effective counter measure. Everyone is concerned when taking about his wallet.
5. No free calls: Very effective. Payment at risk: Interesting idea but too complicated and high operational costs.
6. high
7. It Depends. If the spamer is acting as a commercial/idustrial spamer (commercials) this is not a barrier. In other cases 'money' allways helps to ensure correct behaviour

8. Immediate contact could help, but you must know who to contact and if the caller really leaves a correct number, then tha re-call is wanted. Then if you call back as the only one you're the fool (it's almost the prisoneer's dilemma) IDo not react, won't help (experience from e-mail) except, there are costs for the caller
9. very very effective, this is what drives spam
10. very effective. Break their business model
11. These measures seems to be effective but the problem is, will all user accept this? Telephone Companies are not willing to loose customers due to such measures.
12. Wird kaum möglich sein, wenn sich mit Spam Geld machen lässt.
13. Could be successful if costs to spam are high, but this is not compatible with the trends in VoIP tariffing
14. Der wichtigste Teil.
15. see above
16. Yes, I guess this could be a way. But all the other customers be afflicted with such counters and will not eliminate the real problem.
17. As long as calls are billed and terminations fees exists, it will significantly reduce the potential of VoIP spam. If however an attacker can hack a VoIP system and place calls from that, this will not prevent SPAM
18. No free calls could be helpful. Each call should cost a small amount of money, independent of the duration of the call. This will not hindering non spam calls. But for spammers which want to place thousands of calls it will be expensive to do. Payment at risk seems to be a nice idea, but it depends highly on the callee. If you as callee want to punish the caller you can mark the call as spam and the caller has to pay for it. I think a feedback system with overall rating could be a nice enhancement.
19. Somewhat
20. Quitte effective
21. only "payment at risk" could work because "flat fee / free calls" is a fact (and attracts SPAMMERS) and a marketing issue.
22. Sounds like a good solution, may be a mix of A1, A2, A3, A4 would be the best. In example an addaptiv solution (cheap, quick and testable), which fits to almost every situation!
23. Für Spammers nicht effektiv
24. It can be effective….think of signaling and voice streams…..it is not like email spam. Still people are looking answers in email spam world
25.
26. Effective enough to reach the level we see on PSTN today…
27. Legal measures can only have limited effect since spamming is going beyound political borders.
28. Wenn alles gratis wäre, dann wäre die Motivation wohl für einige geringer, aber das kann ja nicht unsere Antwort sein ;-)) Mit Geld Modellen (auch wenn es kleine Beträge sind) kann schon eine gewisse Steuerung des Kunden / Spammer erreicht werden. Bedingung ist aber, dass die Identität klar ist, und auch nicht so einfach überwindet werden kann.
29. No Free Calls: Ist wirksam gegen normale SPAM-Anrufe. Kann aber mit technischen Mitteln (z. B. Trojanern) umgangen werden.
    Payment at Risk: Wäre gegen normale SPAM-Anrufe wirksam. Eine Implementierung diese Funktion bei allen VoIP- oder Telefonie-Anbietern ist aber nicht in Sicht. Zudem kann auch diese Massnahme mit technischen Mitteln umgangen werden.
30. very effective in case of 'no free calls'
31. Commercial counter measures are not very effective. Again, we base this on the history of e-mail and Spam. For example, 'no free e-mail' was a suggested way to deal with Spam; it was not successful. People do not want to pay per e-mail. The same logic will apply to VoIP. Letting the reciever determine if the call was 'good' or 'bad' to determine if the sender gets paid might work, but it assumes that the sender is using that method to get paid. Maybe the message suggests the user go to a specific web page to purchase a product, for example. This would allow the attacker to be paid, regardless of what the sender chooses to do.
32. I think there must be some safeguards that must be implemented. If you make calls free, then they must be free up to a certain limit (say 1'000 calls per month?). Or if they are totally free then we have to monitor users for high call rates. Also, the service contract should specify that misuse of a phone service is prohibited and that in such case the service may be disconnected pending investigations.
33. Eine gute Methode, sofern das Billing sichergestellt ist.
34. Commercial counter measures are for me hard to implement in environment where the price is really a key factor to gain (keep) customers.
35. Charging will always be more effective for VoIP initiated calls.
36. 99%
37. Kann effektiv sein, wenn die Anwender bereit sind die entsprechenden Kosten zu tragen. Wenn nicht, Nein!
38. In the marketplace "bill and keep" appears to concquer the "calling party pays" schemes making both methods very impracticable for Voip providers.
39. Weniger
40. As long as operators are able to keep the prices 'high' this will prevent voip spamming. But in long-term, commercial counter measures will not be an option

A.1.13. Do you have any additions to the lists provided in Appendix A?

1. -
2. no
3. Nein
4. No
5. no
6.
7. no
8. let me think about…

9. I think it is pretty exhaustive. If you have netflow installed, that is the first log I would look at. correlate with additional statistics, impose trust relationship. RBL don't really work good, 20% suppression rate for EMail spam. ANother way is to analyse the connection behaviour. Often spammers try to connect only once, if there is a failure, they don't try twice (hint, hint)
10. include in ITSP a clause about "appropriate usage" and exclude spamming. This allows legal actions.
11. no
12.
13. What about deep packet inspection?
14.
15. -
16. One issue is that a customer must have the possibility to see which call we have blocked. Moreover countermeasures have to take effect before a call is established. Today it works for E-mail with a separate SPAM-box. At a later date, the customer can fetch out the desired mail or delete it. A further problem is that a call is a time-related message which expected an immediate answer. After all we have to introduce a white list?
17. statistical real time analysis of calls - but its technical in the end trusted relationship / control between carriers at the border of autonomous systems (close or strictly control interfaces to untrusted networks) - technical too, or well, let's call it legal but contractual between two parties
18. no, it is quite extensive list
19.
20. No
21. No.
22. Based on PMG but with additional Billing information
23. nein
24. No
25.
26. The use of SIP protection mechanisms e.g. encryption, cookies, handshake validation etc.
27. No.
28. -
29. –
30.
31. Sandvine feels that the best way to handle VoIP Spam is to approach it in the same way as e-mail Spam: use behavioral technology to identify those who are abusing the system and take appropriate actions against them.
32. Maybe some mechanisms used to mitigate DoS attacks in the IP world can be applied to SIP calls.
33.
34. Not really.
35. To date, we have not seen any issues in this area and therefore have had limited efforts in this area.
36.
37. Nein
38.
39. -
40. No, actually I think they are very good!

A.1.14. What else do you think is important for preventing VoIP Spam?

1.
2. strong originator authentication
3. Ausser den oben erwähnten counter measures fällt mir auf die Schnelle nichts ein.
4. VoIP calls should not be free of charge. It's not an innovation, but it's probably the price to pay for getting rid of spams.
5. End to end protection. This includes Virus (Trojan, Zombie, Rootkit…) protection for PCs in home networks, protection of VOIP phones in the home network, protection of the VOIP web services and their servers, protection of the transmission systems and protocols.
6. That voice SPAM cost money or time or is unsucessful for the initiator
7. Enduser must be able to restrict to a certain degree incoming calls. If this is technical possible, I think that the most impotend part in preventing spam is done.
8. a mix of measurements: tech. counter measurments; law against and punishment for spammers; - termination charges for calls (from othr networks) => will motivate other operators to do something against spam
9. inbuild technical countermeasures ask the security people first before installing a new service DON'T even think of listening to marketing or management if it comes to standards and requirements Involve standard and legal bodies Adress this issue in EU-Project call FP7, I can help there!!!! (hint, hint)
10. -
11. permanently monitoring and exchanging the Knowledge between Operators and VOIP providers
12. man müsste verhindern, dass irgend eine beliebige Station/Endegerät gleichzeitig Verbindungen zu vielen andern (mehr als 3) aufbauen kann.
13. 1) Strong AAA mechanisms to make sure that user connecting to the SC network are who they pretend to be. 2) mechanisms to make sure that source and destination addresses can be trusted
14.
15.

16. - Overall strong end-to-end encryption and authentication. - User authorization with IP address and VoIP accounting data (IP address in Via field). - Efficient server based filtering solutions - VoIP SEAL (SEcure Application Layer gateway). - Limitation o
17. common agreement how to avoid and prosecute such calls among carriers - perhaps a task for standardistation bodies (ITU)? // validated origin identifier when passing a call to an other carrier
18. The counter measures are well explained but it is also important to take care of user acceptrance of these methods in term of intrusivness.
19. Combination of legislation and technology
20. No idea
21. An E2E-view with all involved parties! --> COM / CUC / FRAUD / ABUSE TEAM from FX & MC etc..
22. Suspicious behaviour of Users, recording and adaptation of the SPAM detector according rules!
23. Keine weitere Ergänzungen
24. No
25.
26. To leave some commercial room for email spam!
27. Appropriate security measures and user education.
28. Sensibilisierung der zahlenden Kunden… ihr Anschluss ist sicher, aber zur Unterstützung beachten sie bitte…
29. -
30. no
31. Based on what has been learned from e-mail Spam, behavioral detection is a must to effectively stop VoIP Spam.
32. We have to implement monitoring and alarming functions at an early stage to be able to detect quickly if abnormal use of ressources is occurring somewhere in the network.
33. Die Nutzer von VoIP müssen über SPAM aufgeklärt werden. Sie sollen wissen, wie sie aus Sicht des Nutzers SPAM reduzieren können.
34. It is for me important to show that we are (should be) able to identify SPAMmer and that prosecution will be systematically done. Somehow the same measures as the one existing now for P2P (mp3). Technically we will always fight against SPAM and not prevent it.
35. This will ultimately become an industry issue so addressing this capabilities in industry forums investigating techniques including enhancing signaling and infrastructure to assist. It might also be worth considering the equivalent of a bake off where developers attempt to misuse or run tests on impacts to systems under extreme misuese. Sometimes, spamming can be caused by faulty software as well.
36. do not make calls free of charge (unlimited flat rate is "free of charge for the specific calls") - however… SPIT in the Internet could be a good measure to get people to sign for IMS ;-)
37. Sensibiliserung und Information der Anwender von VoIP Lösungen.
38. in case of legal prosecution it will be important to be able to forensically obtain evidence of calls being made, Also a practicable consumer complaint mechanism will need to be develeoped in order for government agencies to be able to prosecute Voip-spam cases.
39.
40. I strongly believe in a social networking approach on the long-term.

A.2. Questions concerning Legal Issues

A.2.1. Is the new Swiss law on telecommunication (1 April 2007) an effective countermeasure against VoIP Spam?

1. No, It is just the basic framework, but at least it is mentionned
2. Yes
3. Weiss ich nicht. Zu wenig Zeit zum Lesen!
4. Don't know
5. No, Only limited effect. If the spammer sends his messages from a foreign country he will be much harder to catch - if at all possible.
6. No, It will be difficult to identify what is a SPAM call or just a miss typing
7. No, Art 83 (unlautere Massenwerbung.). I think spam is not really fully covered. This text is a beginning but it is not compulsary. (….if technically possible…… opens a wide range of loopholes)
8. Yes, Yes. especially if in addition, nobody can terminate calls in Swiss networks without to pay for. Of course, this does not help if sincere customers computers are cracked and used for spamming.
9. Yes, if, and only if there is an agreement that spammers from foreign countries are subject criminal or civil prosecution. And here we will have a major downturn of the effectiveness of the law. But in principle yes.
10. your link is not accessible due to the word protection… and is wrong…
11. Yes, For SPAMERS coming from Switzerland
12.
13. No, It is a good menace, but I am not sure if it is effective.
14. No, Siehe oben
15. No, This is a global problem.

16. No, It is not very well defined and delegates a possible solution to the telecommunication market. Furthermore there is a big scope left for interpretation. How we will find out if a recipient has agreed to the advertising via telecommunication service or not? Today we us the * headsign in the telephone directory and it doesn't work. Basically I guess, that a "new" telephone service has to operate for the customer a it works today. No additional complexity, no administration of any list. Only blocking set are a possible solution.
17.
18. No, There will be a lot of loopholes that leaves spammers uncatchable especially because of the fact, that law is only a local-one.
19. Not aware of the Swiss law.
20. Sorry, I've no time to read the law
21. Yes, it covers VoIP Spam, but only within Switzerland. It's getting difficult for mistrusted countries.
22.
23. Yes
24. No
25.
26.
27. No, It can only have a limited impact since VoIP spam might be originated from other countries.
28.
29. Yes, VoIP Spam gemäss Definition in Punkt 2.1 in diesem Fragebogen wird vom UWG und damit auch vom Fernmeldegesetz (FMG, SR 784.10) und von der FDV erfasst. Die Bestimmungen sind insbesondere dann wirksam, wenn der Spammer und der Nutznieser des SPAM bzw. SPIT in der Schweiz sind.
30. We will see, but it all depends on whether customers complain and when the spammer is barred by the PTS on what happens next. .
31. No, Sandvine is not a legal service and cannot provide legal advice in terms of the effectiveness of laws. The article seems to talk about how access will be extended to third parties for telephone access and serivces (similar to what has happened in Canada). There is reference to SMS Spam. Although the term 'Spam' is typically associated with e-mail, e-mail is really just the media. The media could be anything: e-mail, SMS, MMS, or VoIP. But that would be up to the courts to decide, we suspect.
32. You have to ask a legal specialist here. I would recommend that you contact someone from Alexander Harte's department. Ask Robert Muralt to organise a meeting.
33. No, Es ist eine Empfehlung und grundsätzlich nur einsetzbar, wenn Anrufe aus Maschinen erfolgen
34. Yes, In this document there is no reference made to the type of transport mechanism used (IP, TDM, ATM) meaning for me that any type of spamming over any type of media is not allowed except if explicitely wanted by the user.
35. In our opinion, this is definitely a movement in the right direction. Those that are out to abuse the technology need to be aware that they will be held liable.
36.
37. Keine Anwort, da ich über den Link das Dokument nicht einsehen konnte
38. Yes, OPTA blieves the provisions are similar to the ones in the European teleciommunications privacy directive.
39. ?
40. didn't have time to read that through yet

A.2.2. Is a Network Operator allowed to do content analysis for the sake fo VoIP Spam protection, without the user's permission?

1. Yes, As long as Data privacy and law is respected, I have no problems. We could make a service out of it. Content analysis for customers who accept it and are willing to pay a monthly fee to have a Spam free VoIP Service
2. No
3. No, Kenne die Gesetzgebung zu wenig, ist nur meine Meinung
4. Don't know
5. No, Not without the user's permission.
6. I think not
7. no answer, i do not know the situation
8. No, content analysis is already done today but a) not for spam prevention and b) only with a judges permission
9. No, no, not really. But if there is a warrant or a criminal case then we have the case of legal interception.
10. No, Telecom Law forbids this
11. Yes, the lnew law asks us to do so, preventing SPAM!
12. No, galube ich nicht
13. Don't know.
14. No, Auf Antrag der B Teilnehmers/ der Behörden kann die Autentifizierung erzwungen werden
15. Yes, Hey, you are asking an IPS guy ;) Content is everything to security.
16. Yes, Sooner or later we have to analys the content to find out recurring events types. With such filters we are in the position to prevent SPIT. (Same approach as today for SPAM)
17. We are not allowed to analyze call content
18. No, Only with the explicit approval of the user/customer.
19. No, That is a privacy issue - what if you discover during content inspection, that someone is going to rob a bank? Do you report it even though content inspection itself was illegal?
20. Yes

21. Yes, text from BAKOM: "Anbieterinnen von Fernmeldediensten müssen: ihre Kunden vor Spam schützen, soweit das möglich ist. Dazu dürfen sie Spam filtern" and "verhindern, dass ihre Kunden Spam senden. Dazu dürfen sie dem Kunden auch den Internetanschluss sperren"
22. No, May be it depends: the user might wish content analysis and may be for it but the user might wish Spam. VoIP as business product should have in my opinion such protection (for me it is QoS). And surely the network operator must guarantee that the content is used only for such spam protection and may be for quality assurance (Data Privacy). The Network Operator could request the user with SLAs to accept or deny such a feature "SPIT protection"
23.
24. Yes, First, It is difficult. Mostly it can be done only on recorded or stored messages, not real-time
25.
26.
27. No
28. No, Einzig die Behörden dürfen den Inhalt eines Streams analysieren. Der Provider stellt nur den Stream zur Verfügung, jedoch niemlas Analysen.
29. Yes, Ja, soweit dies notwendig ist um den Pflichten gemäss Artikel 83 FDV (Unterdrückung unlauterer Massenwerbung durch die Fernmeldedienstanbieter) zu erfüllen. Eine Weitergabe der Inhalte an Dritte ist aber ausdrücklich untersagt (Artikel 43 FMG).
30. No, Datenschutz
31. Again, this depends on the laws in a particular country or area. Sandvine Security Operations addresses this with each of our customers. Typically, we seek their permission to do security audits, and look at any information on their network. As a default position, Security Operations assumes that any data/information obtained during the course of an investigation is kept confidential.
32. No, Again, this is a question for the legal department. I would say that in principle without an order from a judge, it is not allowed to analyse content from conversations. In particular it is very difficult to define a border between what is typological analysis from detailed content analysis (e.g. detecting if a human is speaking or a machine, which may be somehow allowed vs detecting individual words which is probably not allowed)..
33. No
34. No, The only exception I know is Lawfull Interception where the interception must be requested by the Court and of course the user is not informed...
35. Sylantro cannot definitely state whether this is allowed. This has regulatory implications including privacy issues.
36.
37. Yes, Nur so kann er letztendlich gegenüber dem Kunden eine Vertrauenswürdigen Service anbieten.
38. Yes, OPTA would not find automated content analysis objectionable but would object if the user was not aware of the filtering,
39. ? --> Gesetz?
40. No, Operators should never be allowed to do content analysis of phone calls. By the way, I do think the same about e-mail traffic.

A.2.3. Is a Network Operator allowed to block phone calls on their network assuming it is VoIP Spam, without user's permission?

1. No, Assumption is not enough
2. No
3. No, Meine Meinung
4. Don't know
5. No, Not without the user's permission. And: The system must be free of false positives!
6. No
7. Yes, FMG art 83, litera 2 could be a basis for an operator which is willing to do supression. I' am not sure if the suppression von phone calls is included in this law
8. No, but, as long only spam calls are concerned, nobody will explain ;-) I guess, you would also block some wanted calls.
9. Yes, Actually this is already done for "bandwidth optimization" purposes in britain or usa. For IP networks we use attack mitigators, for spam we use access control on the mail gateways, RBLs etc.
10. No, as long as there is no strong law allowing this. Actual law even forbids such invasive actions.
11. No, legal question, I don't think so.
12. Yes, muss aber transparent aufgezeigt werden
13. Probably not
14. No
15. Yes, If we are talking about business only calls yes - as soon as the employee is allowed to receive private calls the game is getting harder and more complex.
16. Yes, If we can certainty guarantee that the phone calls based on SPIT. But there is enough space to be far out.
17. If we discover an abuse, we may disconnect the user based on the contractual relationship with customer.
18. No, see 4.2
19. No, Unfair trade practices
20. Yes
21. Yes, see also answer 4.2. (In the TDM world we block already e.g traffic to dialer destinations or incoming traffic).
22. No, Again it depends on current regulatory decisions. If the user wishes such QoS feature it might be handeled in contracts and SLAs. May be users can be informed about SPIT statistics or alarms to convince them to pay/get free SPIT protection e.g like today with virus protection which a user can rent per monthly fee..But in my opinion a user should still decide whether it is desired or not.

23.
24. Yes, Before users, it is going to affect network operator
25.
26.
27. No
28. Yes, Ich denke Massencalls könnten wohl mit technsichen Erklärungen (Systemgrenzen erreicht, Protect Mechanismen) geblockt werden.
29. Yes, Siehe Artikel 83 Absatz 1 + 2 FDV: Die Anbieterinnen von Fernmeldediensten müssen ihre Kundinnen und Kunden vor dem Erhalt unlauterer Massenwerbung schützen, soweit es der Stand der Technik zulässt. - Sie dürfen unlautere Massenwerbung unterdrücken.
30. No, I do not know
31. Again, this depends on the laws in a particular country or area. Sandvine provides the ability to define a policy that the service provider wishes to have. Part of that policy is the ability to perform specific actions such as shaping, blocking or alerting (among others). The service provider decides what it wishes to occur in the event of specific network conditions or events.
32. Yes, Yes if the service contract includes a statement that VoIP Spam is forbidden, and that a user making VoIP Spam will be disconnected
33. Yes, Wenn auf Grund der Netzdatenanalyse darauf schliessen kann
34. Yes, As far as I know the network integrity has precedence over the "service quality" meaning for me that one operator can suppress phone calls in order to guarantee the integrity of the network; basically no operator is forced to guarantee the service at any time and any place.
35. Sylantro cannot definitely state whether this is allowed. We would expect that contractual language with any customer should have language stating that Swisscom has the right to deny service if the user is found to be abusing their service. Note that if someone else is misusing their account unknowingly, that will complicate the situation.
36.
37. Yes, siehe 4.2
38. Yes, OPTA would only allow this if network integrity were at stake, however, Otherwise the operator should obtain the users consent.
39. Falls blacklisted --> ja
40. No

A.2.4. Is a Network Operator allowed to block phone calls on their transit network assuming it is VoIP Spam, without user's permission?

1. No, Assumption is not enough
2. No
3. No, Meine Meinung
4. Don't know
5. No, The network operator does not know whether the receiver has agreed to receive the call. The NO does not know whether the sender's or the receiver's NO have other measures in place which allow the call.
6. No
7. no answer
8. No, see above
9. No, As far as I know, not
10. No, cf 4.3
11. No, i don't think its allowed
12. weissich nicht
13. could be possible
14. No
15. Yes, Each call costs money.
16. Yes, When prevention should work - yes (same as today for SPAM). But there are so many legal aspects - I don't know..
17. If we dicover an abuse, we may diconnect the originating carrier based on the contractual relationship.
18. No, see 4.2
19. No, see above
20. Yes
21. Yes, see answer 4.2 and 4.3
22. No, see 4.3
23.
24. Yes, just like email spam….. but it should not be false positives
25.
26.
27. No
28. No, Transitverkehr unterliegt besonderen Verträgen. Swisscom hat mit BIC den Internationalen Transitverkher ausgelagert.
29. Yes, Siehe Artikel 83 Absatz 1 + 2 FDV: Die Anbieterinnen von Fernmeldediensten müssen ihre Kundinnen und Kunden vor dem Erhalt unlauterer Massenwerbung schützen, soweit es der Stand der Technik zulässt. - Sie dürfen unlautere Massenwerbung unterdrücken.
30. No, I cannot imagine that this is allowed

31. Again, this depends on the laws in a particular country or area. Sandvine provides the ability to define a policy that the service provider wishes to have. Part of that policy is the ability to perform specific actions such as shaping, blocking and alerting (among others). The service provider decides what they wish to occur in the event of specific network conditions or events.
32. Yes, I guess you can block calls if the called party has lodged a complaint. Actually I am not 100% sure for that…
33. Yes, Wenn auf Grund der Netzdatenanalyse darauf schliessen kann
34. Yes, Same as 4.3
35. Sylantro cannot definitely state whether this is allowed. Again, wording in the original custome contract would probably give Swisscom leverage to address this.
36.
37. Yes, Ja, er muss aber den Kunden informieren.
38. Yes, OPTA would only allow this if network integrity were at stake, however, Otherwise the operator should obtain the users consent and should therefore obtain permission from the transit customer.
39. transit network --> Nein
40. No, I rather think that this should only be done if some exploit is known to spread via voip phone calls, but not for spam

A.2.5. Can a Network Operator in Switzerland nail down a spammer in another country, assuming that spamming is nog allowed in this country (e.g. USA, Netherlands, etc.)?

1. No, Each country has its own legislation and as long as no Global Anti-Spam Agreement exists which is ratified, it will be difficult
2. No
3. No, Gesetz??
4. Don't know
5. No, I believe not. If it were possible it would improve the situation considerably! This question should be researched by our legal services!
6. No, In Switzerland only the swiss law is valid
7. No, will be difficult. Art 83 litera 6 gives some hints. I doubt if this Art 83 is strong enough
8. i don't undertand: do you mean to sue the spammer, (or send an assassin ;-)
9. No, This is what is needed. We here actually try to pin down bot nets who have spamming function and evaluate counterstrike methods for the military. It is possible, it is not legal, here cooperation is needed. What we do is only applicable in case of clear and present danger against CH as a country.
10. No, too expensive to track, usually impossible to find from where the calls are coming (based on actual facts in PSTN)
11. Yes, if you find him and the damage is high enough!
12. weiss ich nicht, denke aber nicht.
13. No, He cannot nail the spammer down, he can just assist in supplying evidence
14. No
15. Yes, Refer to SMTP spam again - but the mentioned countries will not be the source of such attacks
16. No, There are no legal basis for suretyship even the origin is outside from Switzerland.
17. Well, I'm a technician, not a lawyer. We would need to accuse them on the originating country?
18. No, actions could be agreed with the local ones.
19. No, Today PSTN calls can be SPAM.
20. Yes
21. No, I think we can only inform the originating country about SPAM activites.
22. No, I don't think so but it still might be possible depending on local regulatory and current law in the country
23.
24. No, it is very difficult……think of hackers…..
25.
26.
27. No, There will be no legal rights at this moment in time.International regulations should be established.
28. Yes, Ich denke schon, aber wie oben erwähnt, kann das je nach Land ziemlich schwierig werden. In England / USA werden heute jedoch schon Spammer (email) zu empfindlichen Strafen verurteilt.
29. Yes, Da SPAM und SPIT auch in der Schweiz verboten sind, kann er bei sich die selben Massnahmen treffen, wie wenn es sich um einen Schweizer Spammer handelt. Er kann sich zudem an das Statssekretariat für Wirtschaft seco wenden. Dieses ist Teil eines Kontaktnetzwerks der Spamverfolgungsbehörden vieler Länder. Das seco wird dann die Informationen über den Spammer und das durch die Fernmeldedienstanbieterin gesammelte Beweismaterial der zuständigen Behörde im entsprechenden Land übergeben.
30. No, depends on legal agreement between the countriess
31. Again, this depends on the laws in a particular country or area. Sandvine provides the ability to define a policy that the service provider wishes to have. Part of that policy is the ability to perform specific actions such as shaping, blocking and alerting (among others). The service provider decides what they wish to occur in the event of specific network conditions or events.
32. Yes, I don't know really but we should definitely seek international cooperation in this area. Because I assume that spammers located in Switzerland must also be stopped if he is affecting customers in the USA. How does it work with the Internet? I think there is more and more international cooperation regarding the security area, isn't it?
33.
34. No, In an IMS case (i.e between two IMS core networks), the two operators would have to sign an agreement. As part of this agreement I see a clause describing missusage of the network where a user of the partner network doing SPAM should be blocked immediately. Something similar to the current "Malicious Call Tracing".

35. Sylantro cannot definitely state whether this is allowed.
36.
37. Yes, Es wird aber nicht einfahc sein, dies umzusetzen. Die Rechtlichen Grundlagen sind diesbezüglich zu harmonisieren.
38. Yes, Identifying the spammer is very often possible through internation co-operation. Enforcement of the spam legislation in civil cprocedures may, however, not be very effective due to the -often- limited damages that operators occur at the destination end of the spamrun.
39.
40. I have no idea, ask Legal… :-)

A.2.6. Are there any (other) restrictions by the law to implement countermeasures against VoIP Spam?

1.
2. Yes
3. weiss nicht
4. Don't know
5. Yes, Datenschutz (protection of personal data): Can accidentally protect the spammer's identification, can limit the counter measures (restrictions to feedback method).
6. I don't know
7. no answer
8. Yes, if you offend against other laws, e.g. against racial discrimination laws
9. Yes, you are not allowed to actively fight back or remotely disable or DoS his equipment. Acutally a nice invitation for the bad guys without any functioning legal procecuuition in place. Lets see what happenes in future when people realize that country boundaries are void even for VoiP.
10. I don't know, but what about freedom of expression?
11.
12. weiss ich nicht
13. ?
14.
15. No, not sure…
16. Yes, Whitelists / Blacklists is processing of personal data; Infrastructure for consent / withdrawal
17.
18. No, Not aware of others
19. Yes, High penalities.
20. No
21. No, Not known to me.
22. Don't know yet
23.
24. No
25.
26.
27. I do not know.
28. unbekannt
29. No
30. No, I do not know
31. Yes, Again, Sandvine is not legal counsel. That being said, one legal issue would be causing an emergency call (such as a 911 call) to be shaped, blocked, or interrupted in any way or other priority types of calls as defined by the laws in a particular country. Sandvine has the ability to not only shape or block, but also give priority to specific network flows in policy. As an example, although the default policy of a network operator is to shape a specific type of flow, should the flow contain other characteristics, Sandvine could immediately give this 'special flow' high priority.
32. Ask the legal department.
33.
34. No, I am missing experience in that area,
35. Sylantro has no knowledge of this
36.
37. --
38. No, OPTA is not aware of any
39. ?
40. no Idea

A.2.7. Are there effective methods to prove that someone is guilty of distributing VoIP Spam?

1. No, Not known to me so far, but you will tell me different, if I am wrong
2. Yes, traffic logs if authentificated
3. weiss nicht

4. Don't know
5. Yes, Strong Authentication method. Complete log data (whole chain). This would help to prevent SPIT, or would allow to trace back SPITters - as long as the SPITter does not use a hacked account….
6. No
7. no aanswer
8. Yes, e.g. if you have call records and/or statistics. but all legal counter measures only helps in case the spammer is known and not if tha spammer uses zombie computers
9. Yes, you can prove it, by passive hacking methods. But that's it what you legaly can do.
10. No, must go through individual customer complaints…
11. Yes
12. der Ursprung kann wohl auch "vertuscht" werden
13. ?
14.
15. No, AVR and TTS are new technologies that are very flexible. MRCP is also powerful and can allow distributed sources.
16.
17. Customer complaints?
18. No, only if there exists a strong identity mechanism
19. Yes - repeat offender
20. Yes
21. Yes, talk with "Internet Abuse Handling"- Team from Bluewin --> FX-IT-SDY-SE-ABU
22. Yes, Reseach Group at University of Applied Sciences Frankfurt am Main http://www.e-technik.org made a research on that topic for T-Systems where a programm with special algorithm was written to allocate such a user with a big probability. I remember that the program was based on billing information with additional not yet existing fields. It might be that a user is not known about its own behavior of beeing guilty therefore rating can be used and the user (if a user from hosting network operator) might be informed or warned
23.
24. Yes
25.
26.
27. No, I imagine not.
28. Yes, Mit entsprechendem Aufwand können Sapmmer sicher via ihrer IP Adresse rückverfolgt werden. Wie gesagt, in bestimmten Ländern dürfte dies schiwerig werden, oder an der gesetzgebung scheitern.
29. Yes, Ja, aber die Beweisführung ist aufwändig und bedingt oft die Mitarbeit mehrerer Fernmeldedienstanbieter.
30. No
31. What one person thinks is Spam another may think it is not Spam. If a bank sends out a mass VoIP Spam message selling a new credit card for example, many would think this is Spam. If the same bank sends out a VoIP Spam message telling everyone affected that their credit card has been compromised and cancelled and to please call the bank for further instructions, the message would not be considered Spam. A big part of Spam is 'intention'.
32. Yes, There must be a mechanism where a receiver can signal which calls are unwanted. Receivers must lodge complaints, otherwise we cannot react. Also, preventively, we should be able to detect a massive call rate.
33.
34. Good question., What about the case where SPAM has been generated from a user who did not know about it ! (i.e malware infection)
35. Sylantro has no knowledge of this
36.
37. --
38. No, OPTA is not aware of any particular specific methods. In general tracking and tracing to a combination of log-analysis and technical analysis of the calls seems feasable.
39. Yes
40. Yes, Voice recordings, keeping track of call setup information, source /dst IPs etc. Everything together should be enough to prove.

A.2.8. Are there other important legal issues?

1.
2.
3. weiss nicht
4. Don't know
5. I don't know.
6.
7. no aanswer
8.
9. cooperatioin over country boudaries. It only works now by pain infliction.
10.
11.
12. Das Thema muss mit Bakom und UVEK diskutiert werden
13. Internation cooperation of legal authorities
14.
15. reading and analysing voip content is still in question in lots of countries.

16. Protecting content of communication and fact that it has taken place (suppression of communication) Therefore control over any SPIT filter has to be in hands of customer. An other issue is child-welfare.
17.
18. All the important legal issues in Germany have been investigated by the SPIT-AL project.
19.
20.
21. unknown
22. Don't know yet
23.
24.
25.
26.
27. I am not familiar with legal issues concerning VoIP Spam..
28. unbekannt
29. -
30. what if a spammers access is barred, but now he suffers a heart attack and would like to make an emergency call.
31. This depends on the laws of your country. Most countries have not dealt with, or are just starting to deal with, the legal issues surrounding Spam and VoIP Spam. One common method is to have appropriate 'Acceptable-Use Policy' agreements signed by customers when they purhase a particular service. These could outline that Swiss Com has the right to limit or deny service.
32. Ask the legal department
33.
34. Important for me is to know "how strong" and severe is the prosecution.
35. Sylantro has no knowledge of this
36.
37. keine Antwort möglich
38.
39. ?
40.

Appendix B
SPIT Analysis Platform

For this research a platform is set up in order to research the Spammer's methods and to evaluate the anti VoIP Spam products (see *Chapter 6*). This appendix describes the global setup of this platform.

In the research environment (i.e. Swisscom) there was a VoIP network for test purposes which we will refer to as MOI. An installation of the open source IP PBX, Asterisk (www.asterisk.org), is configured to make calls via MOI (see *Figure 18a*). For the installation of Asterisk we used a Trixbox virtual machine image (www.trixbox.org), which is a preconfigured Linux distribution with Asterisk, MySQL (database server) and Apache (web server) installed.

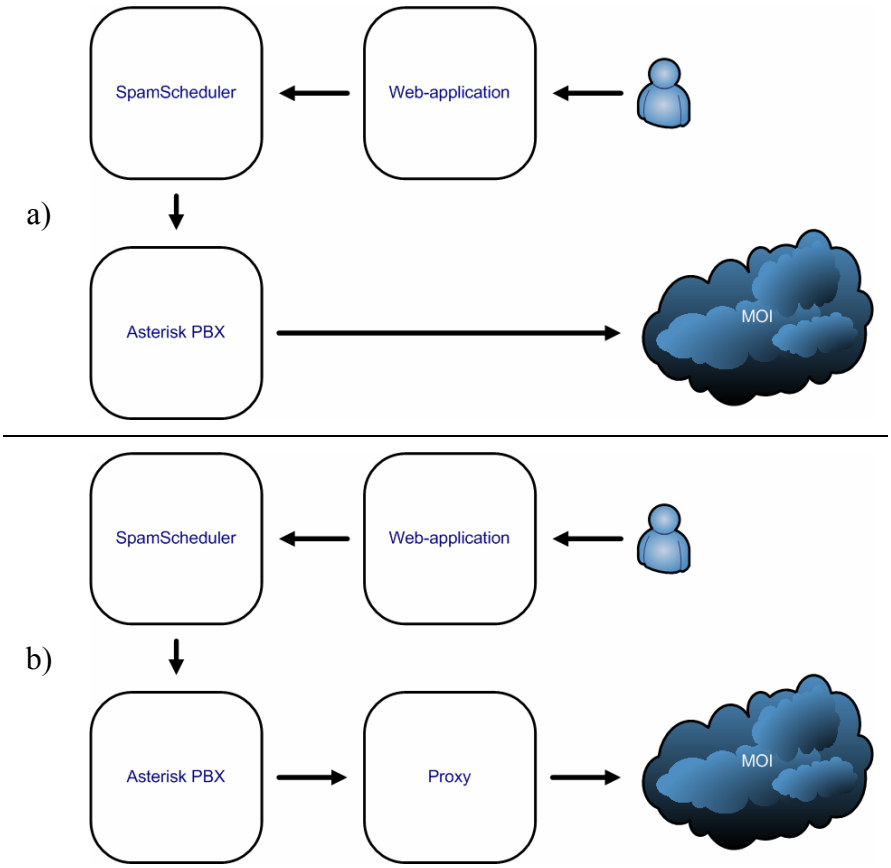

Figure 18: SPIT Analysis Platform without proxy a) and with proxy b)

The program SpamScheduler is specially designed for this research and it can be fed through a TCP connection and communicates with Asterisk via the file system (i.e. the Asterisk spool directory).

A web-application is designed specially for this research and this acts as a GUI for the SpamScheduler program (see *Figure 19*). In this web-application it is possible to select phone numbers, and configure the Spam actions in an easy and straightforward manner. As soon as an action configuration is submitted the application opens a TCP connection to SpamScheduler and executes the appropriate commands.

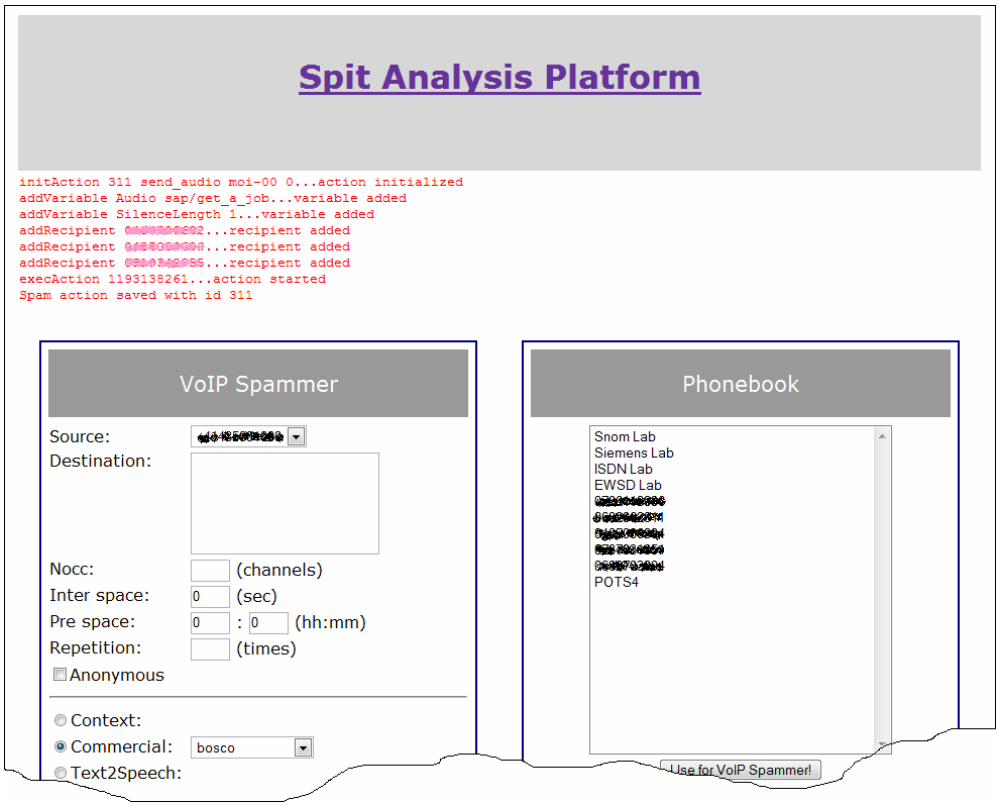

Figure 19: Web-application for the SPIT Analysis Platform

Figure 20 shows an overview of the SpamScheduler program which receives input from the user via the web-application (this part is identified with the A-arrows in the figure), feeds Asterisk via the file system (C-arrows), and receives information about the finished calls via the Asterisk's CDR database (D-arrows). In the SpamScheduler program the command from the web-application are used to compose a Spam action. This action is then placed in the queue (B-arrows) and by the time that it is ready to execute it is executed. This execution results in a number of call files which are written in the spool directory in order to trigger Asterisk to make the phone calls.

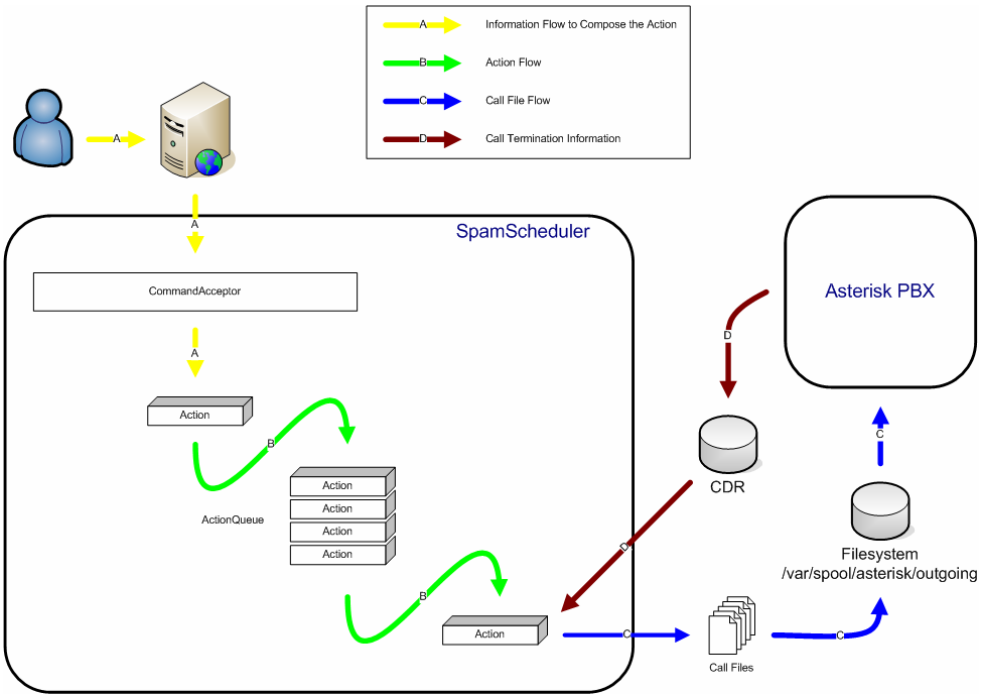

Figure 20: SPIT Analysis Platform architecture

The software products from Eyeball (see *Section 6.1*) and NEC (see *Section 6.2*) are installed on the platform by means of an proxy server (see *Figure 18b*). Both products where installed on a Linux distribution inside a virtual machine.

References

[1] J. Rosenberg and C. Jennings. *The Session Initiation Protocol and Spam*, IETF Internet Draft (work in progress), 9 July 2007

[2] Robert MacIntosh and Dmitri Vinokurov. *Detection and Mitigration of Spam in IP Telephony Networks using Signaling Protocol Analysis*, Alcatel, May 2005

[3] MacMillan English Dictionary for Advanced Learners, 2002

[4] English Wikipedia, *Spam (electronic)*, http://en.wikipedia.org/wiki/Spam_(electronic), Version of July 2007

[5] Dutch Wikipedia, *Spam*, http://nl.wikipedia.org/wiki/Spam, Version of June 2007

[6] German Wikipedia, *Spam*, http://de.wikipedia.org/wiki/Spam, Version of July 2007

[7] Encyclopedia Britannica Online, *Cybercrime – Spam*, http://www.britannica.com/eb/article-235710/cybercrime, Version of July 2007

[8] Britannica Student Encyclopedia, *Computer – Spam*, http://www.britannica.com/ebi/article-234345, Version of July 2007

[9] Stuart Brown, *How Viagra Spam works*, www.modernlifeisrubbish.co.uk, 22 July 2006

[10] Gonzalo Camarillo and Miguel A. García-Martín. *The 3G IP Multimedia Subsystem (IMS)*, Second Edition, 2006

[11] *Why spammers spam – An incursion into the world of spammers*, Norman, March 2005

[12] *Telecommunicatiewet*, Dutch Telecommunication Law, May 2004

[13] J. Rosenber et al. *SIP: Session Initiation Protocol*, IETF RFC 3261, June 2002

[14] International Telecommunication Union, *Packet-based multimedia communication systems*, ITU-T Recommendation H.323

[15] *Global Traffic, Bandwidth, and Pricing Trends and Wholesale Market Outlook*, TeleGeography Research, January 2007.

[16] David Endler and Mark Collier, *Hacking Exposed – Voice over IP Security Secrets & Solutions*, ISBN 0072263644, 2007

[17] Lawrence Lessig, *The Future of Ideas – The Fate of the Commons in a Connected World*, 2001

[18] H. Tschofenig et al, *A Framework for Reducing Spam for Internet Telephony*, IETF Internet Draft (work in progress), 14 June 2007

[19] J. Callens, *SPAM – Studie omtrent de problematiek, gevolgen en juridisch/technische maatregelen ter bestrijding of voorkoming*, Diploma Thesis, 2006

[20] English Wikipedia, *Affiliate Marketing*, http://en.wikipedia.org/wiki/Affiliate_marketing, Version of 14 August 2007

[21] J. Van Meggelen, J. Smith and L. Madsen, *Asterisk – The Future of Telephony*, O'Reilly Media, 2005

[22] *The State of Spam – A Monthly Report*, Symantec, July 2007

[23] Navtej Singh, *IMs, VoIP and Spam*, McAfee Avert Labs Blog, 22 December 2006
[24] Kurt E. Berger, *SPAM: It's not just for breakfast anymore*, July 2004
[25] Peter Brockmann, *The Spam Index Report – Comparing Real-World Performance of Anti-Spam Technologies*, Brockmann & Company, July 2007
[26] S. Niccolini et al, *SIP Extensions for SPIT identifications*, IETF Internet Draft (work in progress), 23 February 2007
[27] S. Niccolini et al, *Signaling TO Prevent SPIT (SPITSTOP) Reference Scenario*, IETF Internet Draft (work in progress), 11 January 2007
[28] N.J. Croft and M.S. Oliver, *A Model for Spam Prevention in IP Telephony Networks using Anonymous Verifying Authorities*, University of Pretoria, South Africa, April 2005
[29] Y. Rebahi and D. Sisalem, *SIP Service Providers and The Spam Problem*, Fraunhofer Institut Fokus, Germany, June 2005
[30] *Bluewin PHONE*, Product Webpage, de.bluewin.ch/services, Version of 23 October 2007
[31] *Business Connect Professional*, Product Webpage, www.swisscom-fixnet.ch/fx/geschaeftskunden/index.htm, Version of 23 October 2007
[32] *[VOIPSEC] Confirmed cases of SPIT*, VOIPSEC Mailing list, VOIP Security Alliance, March 2006
[33] *ACMA media release 86/2007*, Australian Communications and Media Authority, 23 July 2007
[34] *Security Threats January-June 2007*, Marshal Threat Research & Content Engineering Team, July 2007
[35] *Know your Enemy: Tracking Botnets – Source Code*, Honeynet Project, Version of 17 February 2005
[36] *Press Release – Over 1 Million Potential Victims of Botnets Cyber Crime*, FBI, 13 June 2007
[37] *[VOIPSEC] VoIP bots for SPIT available for research*, VOIPSEC Mailing list, VOIP Security Alliance, May 2007
[38] *Gevangenisstraf en geldboetes voor computerhackers*, Press Release, Public Prosecution Service (Dutch: Openbaar Ministerie), 30 January 2007
[39] *Voice over IP & IP-Telephony*, MarketCap B.V., September 2006
[40] *Data protection: "Junk" e-mail costs internet users €10 billion a year worldwide – Commission study*, Press Release, European Union, 2 February 2001
[41] H. Tschofening and E. Leppanen, *Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) based Robot Challenges for the Session Initiation Protocol (SIP)*, IETF Internet Draft (work in progress), 2 July 2007
[42] *Cisco CallManager Features and Services Guide*, Release 4.0(1), Cisco System Inc., 2003
[43] Michael Pantridge, *VOIP Spam Counter Measures*, Technical University of Denmark – Master Thesis, 2006
[44] J. Quittek et al, *Detecting SPIT Calls by Checking Human Communication Patterns*, NEC Europ Ltd., 28 February 2007
[45] *The Marketer's Guide To Successful Email Delivery*, ThinData The Email Authority, 2007

[46] J. Rosenberg et al, *A Framework for Consent-Based Communication in the Session Initiation Protocol (SIP)*, IETF Internet Draft (work in progress), 12 June 2006
[47] *ITU Survey on Anti-Spam Legislation Worldwide*, ITU, 2005
[48] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, *The EigenTrust Algorithm for Reputation Management in P2P Network*s, WWW2003, May 2003
[49] Frank geht ran, www.frankgehtran.de, Version of September 2007
[50] Ram Dantu and Prakash Kolan, *Detecting Spam in VoIP Networks*, Dept. of Computer Science and Engineering, University of North Texas, Denton, Aug 2005
[51] *Deutsche Internet-Telefonzentrale erhält Schutzschild gegen Spit-Angriffe*, Press Release, Toplink GmbH, January 2005.
[52] *SIPassure Product Brochure*, BorderWare Technologies Inc. 2006
[53] *ETM Product Brochure*, SecureLogix Corporations, 2005
[54] *A SPIT prevention system for voice-over IP telephony services*, Voice & Data Security (VoDaSec) Solutions, March 2007
[55] *Eyeball AntiSPIT Technology*, White Paper, Eyeball Networks, 2005
[56] Roman Schlegel et al, *Spam over Internet Telephony (SPIT) Prevention Framework*, NEC Europe Ltd. November 2006
[57] Stefan Liske et al, *Implicit Reputation in a Payment Integrated SIP Network*, University of Potsdam, Department of Computer Science, May 2007
[58] Vrouw sterft door online gekochte neppillen, News Item, Security.nl, 23 March 2007
[59] M. Handley et al, *SDP: Session Description Protocol*, IETF RFC 4566, July 2006
[60] H. Schulzrinne, *RTP: A Transport Protocol for Real-Time Applications*, IETF RFC 1889, January 1996
[61] P. Faltstrom, *The E.164 to Uniform Resource Identifier (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, IETF RFC 3761, April 2004
[62] M. Mealing et al, *The Naming Authority Pointer (NAPTR) DNS Resource Record*, IETF RFC 2915, September 2000
[63] J. Franks et al, *HTTP Authentication: Basic and Digest Access Authentication*, IETF RFC 2617, June 1999
[64] *Storm botnet serves-up a diet of fast-flux spam*, Monthly Report, MessageLabs Intelligence, August 2007
[65] Jonathan B. Postel, *Simple Mail Transfer Protocol*, IETF RFC 821, August 1982
[66] *Skype API Reference*, Skype, Version of October 2007
[67] *Bundesgesetz gegen den unlauteren Wettbewerb (UWG)*, Swiss Law against Unfair Competition, 1 April 2007
[68] *Verordnung über Fernmeldedienste (FDV)*, Swiss Regulation for Telecommunication Services, 1 April 2007
[69] *Directive 2002/58/EC*, the European Parliament and of the Council of the European Union, 12 July 2002
[70] Dongwook Shin et al, *Progressive Multi Gray-Leveling: A Voice Spam Protection Algorith*, September/October 2006

[71] Florian Hammer et al, *Elements of Interactivity in Telephone Conversations*, Telecommunication Research Center Vienna, July 2004
[72] *Stage 3 description for number identification supplementary services using DSS 1: Malicious Call Identification (MCID)*, Recommendation Q.951.7, ITU-T, June 1997
[73] *Sipera IPCS 410 and IPCS 510*, Datasheet, Sipera Systems, August 2007
[74] Paul Hazlett et al, *SER – Getting Started*, ONsip.org, May 2006
[75] *Only drugs can prove deadly: coroner*, News Item, The Vancouver Sun, 21 March 2007
[76] Mohamed Nassar et al, *Holistic VoIP Intrusion Detection and Prevention System*, LORIA – INRIA Lorraine and NEC Europe Ltd., June 2007
[77] G. Dawirs et al, *Authorization Policies for Preventing SPIT*, IETF Internet Draft (work in progress), 26 February 2007
[78] Adrian Rishi Madhosingh, *The Design of a Differentiated Session Initiation Protocol to Control VoIP Spam*, Florida State University, 2006
[79] Laura L. Frieder and Jonathan L. Zittrain, *Spam Works: Evidence from Stock Touts and Corresponding Market Activity*, Purdue University and Oxford Internet Institute, August 2006
[80] *Internet Protocol – Darpa Internet Program Protocol Specification*, IETF RFC 791, September 1981
[81] *VoIPblock Anti-SPIT (Voice Spam)*, Product Webpage, www.voipshield.com/products/voipblock.html, Version of 3 November 2007
[82] Stefan Liske et al, *SPIT-Erkennung, -Bekanntgabe und -Abwehr in SIP-Netzwerken*, University of Potsdam, Department of Computer Science, February 2007
[83] *Stock spammers pump up the volume with MP3 files*, News Item, Sophos, 18 October 2007

Abbreviation List

3GPP	3rd Generation Partnership Project – Collaboration between groups of telecommunication associations..
BAKOM	BundesAmt für KOMmunikation (*Section 3.1*).
BSN	Borderware Security Network – „BSN is a real-time reputation service that monitors and identifies threats across multiple Internet communication protocols“ (bsn.borderware.com).
CAPTCHA	Completely Automated Public Turing test to tell Computer and Humans Apart (*Section 5.1.4*)..
DNS	Domain Name System – The DNS is used to translate human-readable hostnames into IP addresses, which are needed for network equipment to deliver the information.
FAR	False Accept Rate (*Section 3.5*).
FDV	Verordnung über Fernmeldedienste – Swiss law for telecommunication services (see *Section 4.9.2*).
FN	False Negative (*Section 3.5*).
FP	False Positive (*Section 3.5*).
FRR	False Reject Rate (*Section 3.5*).
GUI	Graphical User Interface – The graphical part of a piece of software which directly interacts with the user.
IM	Instant Messaging – A form of real-time communication between multiple users based on text messages.
IMS	IP Multimedia System – A specification from the 3GPP for delivering multimedia on an IP network.
IP	Internet Protocol – IP is a data-oriented protocol for communication via a packet-switched network. IP is the Internet’s main protocol.
ISIM	IP multimedia Subscriber Identity Module (*Section 7.1.2*).

ISP	Internet Service Provider – The organization which provides internet access to their customers.
IVR	Interactive Voice Response (*Section 3.4*).
LAN	Local Area Network – A computer network covering a small area (e.g., home, office).
NAT	Network Address Translation – NAT is a technique for sharing a single IP address by multiple hosts in an IP network.
NGN	Next Generation Networking – The architectural evolution of telecommunication systems from circuit switched to packet switched networks (e.g. IP networks).
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit (*Section 3.1*).
PBX	Private Branch eXchange (*Section 3.4*).
PMG	Progressive Multi Grey-levelling (*Section 5.1.3*).
PSTN	Public Switched Telephone Network (*Section 3.4*).
RFC	Request For Comment – A document addressing one of IETS's internet standards.
RTP	Real-time Transport Protocol (*Section 3.2.3*).
SDP	Session Description Protocol (*Section 3.2.3*).
SER	SIP Express Router (www.iptel.org) - Multifunctional SIP server (i.e. registrar, proxy, and redirect server) licensed under the open-source GNU license.
SIM	Subscriber Identity Module (*Section 3.2.4*).
SIP	Session Initiation Protocol (*Section 3.2.3*).
SPIT	SPam via Internet Telephony (*Section 3.3*).
TCP	Transmission Control Protocol – TCP is one of the core protocols of the Internet Protocol suite. TCP provides reliable communication and could for example be used for file-transfer and e-mail.
UICC	Universal Integrated Circuit Card – Removable smart card used in cellular telecommunication to store the SIM.

UDP User Datagram Protocol – UDP is one of the core protocols of the Internet Protocol suite. UDP does not provide reliable communication and could for example be used for streaming audio/video.

USB Universal Serial Bus – A standard for communication between devices.

UWG Bundesgesetz gegen den unlauteren Wettbewerb – Swiss law against unfair competition (see *Section 4.9.1*).

VOIP Voice over IP (*Section 3.2*).

List of Tables and Figures

Index