Project no.:	**COOP-32720**
Project full title:	**SPam over Internet telephony Detection sERvice**
Project Acronym:	**SPIDER**
Deliverable no.:	**D2.1**
Title of the deliverable:	**SPIT Threat Analysis**

Contractual Date of Delivery to the CEC:	31.01.2007
Actual Date of Delivery to the CEC:	
Author(s):	Y. Rebahi, S. Ehlert, M. Theoharidou, J. Mallios, S. Dritsas, G. F. Marias, L. Mitrou, T. Dagiuklas, M. Avgoustianakis, D. Gritzalis, B. Pannier, O. Capsada, J. Markl
Participant(s):	Fokus, AU, VozTelecom, Nextsoft, Eleven
Work package contributing to the deliverable:	WP2
Dissemination level:	Public
Version:	Final
Total number of pages:	33

Abstract:
SIP based Voice over IP (VoIP) is an emerging technology that will certainly suffer from the SPAM problem in the future. In this deliverable, we try to better understand the SIP SPAM problem in order to define the adequate mechanisms for protecting the SIP infrastructures. In fact, we have focused on providing accurate and useful information about prior SIP SPAM activities that could help prevent some future ones from occurring. One of the key findings of this study is the identification of the SIP protocol vulnerabilities that can be used by the spammers to generate SPAM "attacks". This process, known as SPIT threat assessment, takes these findings one step further by identifying the eventual SPIT scenarios and evaluating them. This document is intended to provide, not only for the SPIDER consortium but for all people interested in this area, a guide for developing appropriate techniques that can help in SPIT prevention.

Keyword list: SIP, VoIP, SPAM, SPIT, Regulations, Threat Analysis, Assessment, Statistics, Prediction, SIP vulnerabilities

Table of contents

1 Introduction

The session Initiation Protocol (SIP) is becoming the first standard for managing IP multimedia sessions. Similar to most of email protocols currently used, SIP can suffer from the spam problem. The latter refers in general to any unsolicited information sent to any recipient without its consent. For convenience purposes, we will make no difference between the terminologies SIP SPAM and SPIT (SPAM over Internet Telephony) along this paper. SIP is still an emerging technology, however, it is more reasonable to address the SPAM problem right now than wait until this problem becomes serious. As a consequence, the risk from such acts must be assessed to determine the adequate measures to be used for facing this threat. This assessment will also allow us to check whether the existing used security measures are efficient or need improvement.

Threat analysis is the first step in risk assessment for SPIT. It is used to identify the sources and types of threats and their likelihood. Once a threat is identified, its corresponding scenarios are analyzed, i.e how this threat could be realized. The results of this analysis are used to assist in making decisions on the levels of the prevention and detection techniques that are needed.

The current deliverable describe a threat analysis for SIP SPAM. We start by fixing the "SPAM" terminology from a technical point of view. The general meaning of "SPAM" is discussed and then applied to the VoIP case. After that, we investigate how regulations, especially the European ones, look at this threat. In fact, the SPAM problem for VoIP is still in an infantile stage, so no real "legal work" can be found in the literature expect some general "laws" that can be extrapolate to the SIP SPAM case. This lack of information has also made harder the task of gathering SIP SPAM statistics for eventual studies or prediction. In spite of this fact, the email and PSTN SPAM cases are studied and the results are applied to the case of VoIP according to the possible existing similarities. As spammers will certainly exploit SIP vulnerabilities to generate unsolicited calls and Instant Messages (IMs), a detailed description of these vulnerabilities as well as the way they are used for creating SPAM is provided. In addition to the identification of the SPIT threats, the motivation behind sending spam and the spammers' tools are discussed. Finally, the defined SPIT threats are assessed according to some metrics based on parameters such as the amount of difficulty needed to generate spam from a given threat and the impact of this SPAM activity on subscribers and organizations.

2 Spam-General Overview

2.1 Generalities

In general, Spam refers to any unsolicited information that is sent to you without your permission. According to some studies [1], half of the received spam information is related to money, for instance, advertisement, debt reduction and gambling opportunities. One fourth of spam is related to stocks market, 10% is health-based and about 5% is pornography-related. The rest of spam spans a wide variety of topics, for instance, new jobs openings, cheap university diplomas, etc [1].

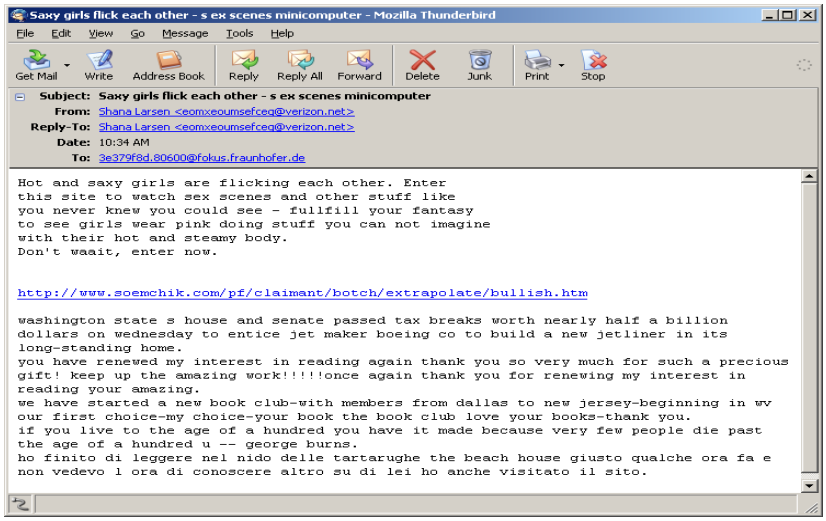

Figure 1: a sample of email spam

As the spam information is without interest for the majority of people to whom this information is sent, the spammers try to utilize widely used carrier tools that have extremely low cost in order to guarantee high gains. Few years ago, Fax was the main tool used for sending spam, however, the current favorite tools utilized for transmitting spam information are emails (Figure 1) and phone calls. Actually, 10s TV advertisement can cost more than 1000$, however, a spam over one million email address costs less than 25$. For the future, IP telephony seems to be the adequate means for sending spam because of the low cost of the Internet connections and the convergence of data and voice provided by the corresponding voice over IP protocols.

Although, various anti-spam techniques are deployed everywhere, the spam problem still persists. The major reasons for that are the following,

- Earlier in this section, we tried to provide a general definition of spam. However, the latter is a subjective notion on which it is not completely agreed and which is difficult to detect by means of software. In spite of the fact, that there is unanimity on considering drugs, pornography and viruses related messages as spam, a commercial related message (software sales) or a message advertising a job opening can be without interest for a user, however, it might be of great interest for another one. In addition, one user (or company) may tolerate a small amount of false positive messages (non-spam messages that are considered as spam) in order to block all the spam messages even before seeing them. However, another user does not tolerate any message loss even the spam that he receives is significant. A third user might tolerate false positives (or negatives: spam messages that are considered as non-spam) related to some kind of spam (mortgage rates) and does not tolerate in any case false positives (or negatives) related to another kind of spam, for instance pornography
- Spam techniques also evolve. The spammers, motivated by financial gains and low costs for spam deployment, learn how the current anti-spam tools work and continuously adopt new techniques that can bypass them

2.2 Legal issues

2.2.1 Definitions

2.2.1.1 Defining spam from a legal point of view

Although the term " spam" is used in policy texts, surveys or media reports there is no commonly held legal definition of the term. Since the beginning of the 90's the term spam became commonly used to describe "any received message that is unwanted by the recipient", often consisting of advertisements for products and services[1], an approach criticized by the Anti-Spam Task Force of OECD as "too broad and simplistic"[2] as it neither specifies the messaging medium nor differentiates spam from legitimate practices. Most worldwide proposed definitions of spam refer to the following elements: unsolicited, bulk, commercial.

In its Communication "on unsolicited commercial communications or spam" the European Commission aptly notes that the term is more used as defined: the term is neither defined nor used by the relevant Directives. In official EU Documents spam is defined as "the repeated mass mailing of unsolicited commercial messages by a sender who disguises or forges his identity"[3] or the "sending in bulk of unsolicited advertising marketing material via e-mail"[4]

The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)[5] refers to "unsolicited communications" by "electronic mail" "for the purposes of direct marketing", which – according to the European Commission "taken together will, in effect, cover most sorts of spam"[6].

A first critical component of all definitions seems to be the term "unsolicited". In an opt-in system, like the system adopted by the EU, unsolicited communications, i.e. communications sent to users without their prior consent, are illegal. In an opt-out system, there are unsolicited legal communications (before recipient's opt out) and unsolicited illegal communications (after recipient's opt out).[7]

As "communication" is defined "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communication service"[8]. Specific attention deserves the concept of "electronic mail": According to the definition[9] electronic mail is "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient". By this concept is covered not only traditional SMTP-based "e-mail", SMS or MMS but also "any form of electronic communications,

[1] For the history of the term IViR, Regulating spam – Directive 2002/58 and beyond (2004)

[2] OECD-Directorate for Science, Technology and Industry – Spam Task Force, Anti-spam regulation, DSTI/CP/ICCP/SPAM (2005)10/FINAL

[3] Commission of the European Communities, Unsolicited commercial communication and data protection – Summary of Study findings (2001)

[4] Data Protection Working Party(DPWP), Privacy on the Internet-Glossary (2000)

[5] Official Journal L 201 , 31/07/2002 P. 0037 - 0047

[6] Commission of the European Communities, Communication on unsolicited commercial communication or "spam" , COM (2004) 28 final, January 2004

[7] N. Lugaresi, European Union vs. Spam: A Legal Response,2005

[8] Article 2 (d) of the Electronic Privacy Directive

[9] See Art 2 (h) of Electronic Privacy Directive

where the simultaneous participation of the sender and the recipient is not required"[10]. Included are inter alia messages left on answering machines, voice mail service systems, including on mobile services, "net send" communications addressed directly to an IP address[11].

The reference to "a finite number of parties" has to be interpreted as aiming at "point to point communication."[12]Even if the use of bulk seems to be a defining element of spam, which is usually associated with sending unsolicited mails in large numbers[13], the provisions of the Directive do not presuppose a large or a minimum amount of e-mail sent. This approach is understandable. A fixed threshold would be circumvented by spammers and would lower the level of protection.[14] Even a single mail is to be considered as spam as the consequences for a particular recipient remain the same, regardless the number of sent messages. The European approach is based on the consent principle and not on the quantity of electronic mails[15].

Usually spam is related to the commercial nature[16] of the communication/content. However Art. 13 of the E-Privacy Directive does not use the term commercial, but the "direct marketing purposes". A description of "direct marketing purposes" is included neither in the general (Framework Data Protection Directive 95/46/EC) nor in the specific European legislation (E-Privacy Directive). A reference is included in Recital 30 of the Framework Data Protection Directive, describing marketing purposes as those "carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example". A broad approach is adopted by FEDMA (Federation of European Direct Marketing) in its Code of Practice for the use of personal data in direct marketing[17], which defines direct marketing "as the communication of whatever means of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals". The DPWP[18] is of the Opinion that the provisions of Art. 13 of Directive 2002/58/EC cover "any form of sales promotion, including direct marketing by charities and political organisations (e.g. fund raising)"[19]. However, it is to be very carefully considered whether a political statement could be labeled as "spam" as such a definition could implicate in the freedom of speech and political marketing.

2.2.1.2 Spam in relation to VoIP

[10] European Commission, Communication on unsolicited communications or "spam" . See also Recital 40 of Directive 2002/58/EC
[11] DPWP, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (WP 90 – February 2004)
[12] IviR, 25
[13] See J. Hladjk, Effective EU and US approaches to spam? Moves towards a coordinated technical and legal response – Part I, Communications Law, Vol. 10, No 3, 2005, pp. 71-
[14] Lugaresi, D. E. Sorkin, Technical and Legal Approaches to Unsolicited Electronic Mail, 35 USF Law Review 325 (2001) pp. 325-384
[15] IviR, …
[16] The European Commission uses in its Communication (2004) the term spam as a "shortcut for unsolicited commercial electronic mail"
[17] This Code has been approved by the DPWP (WP 77 –2003). http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp77-annex_en.pdf
[18] The Data Protection Working Party is composed of a representative of the supervisory authority or authorities designated by the Member States and of a representative of the authority or authorities established for the European institutions and bodies and of a representative of the Commission. Art. 29 of the Framework Data Protection Directive (95/46/EC)
[19] DPWP, Opinion 5/2004

Concerns have been raised in respect of telemarketing, Internet telephony (Voice over IP (VOIP)) and short range wireless communications (in the style of Bluetooth/wireless networking devices). As the OECD Spam Task force points out, 3G and 4G telephony may further encourage the convergence of messaging formats. The increasing take up of Voice over IP (VOIP) may further accentuate convergence of messaging formats.[20].

A list of communications or communication means could not be exhaustive but subject to revision in view of technology and market developments. In developing an anti-spam regulatory approach, it is useful to recognise that messaging formats will merge or evolve, and unforeseen messaging media may arise.[21] The definition of electronic mail in the Directive 2002/58/EC is consciously broad and intended to be technology neutral[22].

According to the Commission the legal framework has to ensure that services are regulated in an equivalent manner and consumers/users should get the same level of protection regardless of the technology used.[23] Consequently the above-adopted definition of spam is applicable to any form/means of spamming. The legal provisions, presented in this text apply mutatis mutandis to similar technologies with different specifications. The forms and means of spamming are however of critical importance in relation to the methods of detection and prevention of spam and the respective legal restrictions (communications secrecy, privacy etc.).

2.2.1.3 The notion of "personal data"

The applicability of data protection rules relies on the processing of "personal data". Personal data mean any information relating to an identified or an identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to its physical, physiological, mental, economic, cultural or social identity [Art. 2 (a) of Framework Data Protection Directive]. These criteria refer to the relevant agent of identification, the ease and the precision of the identification. A person shall not be regarded as "identifiable" if the identification requires an unreasonable amount of time, cost and manpower[24].

Direct identification is possible if for example an e-mail address contains one or more of identifiable factors, such as a name, so that the person to which the data relate can be identified without the use of the a third source.[25] Some authors stress the attention to the requirement, that the identification must lead to "flesh and blood person" and not to a simple online identity, which does not necessarily coincide with the legal, off-line one.[26].

Phone numbers allow indirect identification of subscribers through the use of reverse directories as well as through electronic communications services providers. Indirect

[20] OECD-Directorate for Science, Technology and Industry – Spam Task Force, Anti-spam regulation, DSTI/CP/ICCP/SPAM (2005)10/FINAL

[21] OECD-Directorate for Science, Technology and Industry – Spam Task Force, Anti-spam regulation, DSTI/CP/ICCP/SPAM (2005)10/FINAL

[22] See Recital 4 of the Directive 2002/58/EC

[23] Communication from the Commission to the European Parliament concerning the Common Position of the Council on the adoption of e-Privacy Directive (SEC/2002/0124 final)

[24] Council of Europe, Recommendation No R (85) 20 of the Committee of Ministers to Member States on the protection of personal data used for the purposes of direct marketing. Appendix with Guidelines.

[25] IViR Report, Lugaresi

[26] Dana Irina Cojocarasu, Anti-spam Legislation between Privacy and Commercial Interests, RDEGNT WEB N.2, Aprile-Giugno 2006

identification allow also IP addresses, which can be traced back to a computer and through the provider consequently to a subscriber. Even if the link between subscribers and users is in the case of IP address less strong than by e-mail addresses and phone numbers, most IP addresses can be tied to a log-in and may qualify as personal data.[27]

2.2.1.4 Spam as violation of the rights to privacy and to data protection

The European legislation provides safeguards in relation to the receipt of unsolicited communications not only because they may impose burden and/or costs to the recipient but mainly because unsolicited communications affect fundamental rights of the individual.[28] Spam is deemed to be an invasion of privacy.[IviR]. The fundamental right of privacy, anchored in Art. 8 of the European Convention of Human Rights as well as in the Charter of Fundamental Rights of the European Union [Art. 7 (privacy) and Art. 8 (data protection)] encompasses informational privacy, relational privacy and freedom of communication in the meaning of privacy/secrecy of communications. Informational privacy (or right to informational self-determination) relates to the individual's right to decide autonomously, whether and which personal data can be communicated to others or/and processed by them. Affected is also the so-called relational aspect of privacy, i.e. the right to determine, which communications one wishes to receive or not[29].
Primarily, unsolicited communications infringe privacy in its narrow and visible sense,i.e. through the illegal intrusion into computers and servers and in the final analysis into the private sphere of the person.[30] Further, spam and the respective unlawful collection and use of personal data. deprives individuals from their capacity to determine what information about him/her will become known to the others, affecting the right to self-determination. Another dimension of this right is the control over the flow of information entering their private sphere[31].
VoIP spam (in the forms of "call spam", IM spam, Presence Spam) differs from other "traditional" forms of electronic communications (e.g. e-mail) in that is significantly more obtrusive and intrusive, as a phone will actually ring with every spam message, possibly after midnight.[32]

2.2.2 Regulatory Framework

Spam is a "horizontal" issue, touching upon different aspects of electronic communication services, consumer protection, privacy and security, at national and cross-border levels. Accordingly, the legal framework that has been put in place is complex, owing in particular to the several national public and private enforcement agencies that are dealing with this topic and the need to cover different types of spam.

---

[27] IViR Report, 45
[28] Recital 40 of the e-Privacy Directive
[29] Some authors, like J. Kabel (in its article Spam: A Terminal Threat to ISPs?, Computer und Recht International 2003- 1: 1-5), are of the opinion that in the first place affected is the privacy in its relational aspects and not the informational privacy or the privacy of communications. Kabel perceives relational privacy as a category of freedom of expression, in the concrete case the right not to receive information.
[30] Recital 24 of the e-Privacy Directive states that "terminal equipment of users and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms"
[31] N. Lugaresi, European Union vs. Spam: A Legal Response (2005)
[32] J. Posegga/J. Seedorf, Voice over IP: Unsafe at any Bandwidth? (2005)

2.2.2.1 European Union

2.2.2.1.1 Distance Selling Directive

The Directive 97/7/EC on the Protection of consumers in respect of distance selling was the first European legal text to protect consumers from unsolicited communication. While the Directive requires prior consent of the consumer for the use of automated calling systems without human intervention as means for concluding a contact [Art. 10 (1)], the use of "other means of distance communication, which allow individual communications", is allowed only where there is no clear objection from the consumer. The latter provision seems to have implied an opt-out regime for other unsolicited communications[33].

2.2.2.1.2 E-commerce Directive

The Directive 2000/31/EC on certain legal aspects of information society services, in particular e-commerce, in the internal market (Directive on electronic commerce), has as first explicitly mentioned electronic mail as an example of unsolicited communication. The e-commerce Directive provides for the protection of users from such communications, stating that – when commercial communications are permitted – these communications shall be identifiable clearly and unambiguously upon receipt of the message [Art. 7 (1)]. This can be achieved through a label like ADV (advertisement) at the header of the message. The labeling requirements apply next to the requirements of the e-Privacy Directive. Art. 7 (2) provides for the obligation to consult and respect opt-out registers regarding unsolicited commercial communication by electronic mail[34].

2.2.2.1.3 (Framework) Directive 95/46/EC on the protection of personal data

The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Framework Data Protection Directive) provides the framework for the lawful and fair processing of personal data. Directive 95/46/EC applies to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of the e-privacy Directive, including the obligations of the controller and the rights of individuals[35]. The conditions, laid down in the Directive, for the processing of personal data must be respected in the context advertising. These provisions include further the requirements to provide information to the individuals about the identity of the controller, the purpose of processing, the rights of access and rectification etc. A critical requirement refers to the lawful and fair collection and further processing of personal data, which invokes major problems in relation to the so called e-mail harvesting, which does respect neither the finality principle (purpose limitation) nor the obligation of information.[36]

[33] M.Y. Schaub, Unsolicited mail. Does Europe allow spam?, Computer Law and Security Report Vol. 18 No 2, pp. 99-105 (104)

[34] A provision, which has been interpreted as the Directive leaving the Member States the choice between the opt-in and opt out regime although the Directive does not deal with the question of consent.

[35] Recital 10 of Directive 2002/58/EC on privacy and electronic communication (e-privacy Directive)

[36] DPWP, Opinion 5/2004 on unsolicited communications for marketing purposes

2.2.2.1.4 Directive 2002/58/EC on privacy and electronic communication (e-privacy Directive)

The so-called e-privacy Directive particularises and complements the abovementioned Framework Directive for the protection of personal data and other fundamental rights in the electronic communications sector [Art. 1 (2)]. Directive 2002/58/EC replaced the Telecommunications Privacy Directive (97/66/EC).The general provision on unsolicited communication has been laid down in Art. 13, which has been the result of a compromise between the competing interests.

Communications for direct marketing purposes are definitely placed under an opt-in regime (Art. 13), which is based on prior consent of subscribers, which has the meaning laid down in the Framework Data Protection Directive, i.e. it has to be "a freely given, specific and informed indication of its wishes"[37]. Consent may be given by any appropriate method enabling a freely given, specific and informed indication, including by ticking a box when visiting an Internet website. Consent given on the context of main contract must respect the specific legal requirements. Implied consent is not compatible with the definition of context, which means that pre-ticked boxes, are not compatible. Clearly indicated to the subscriber should be the purposes, e.g. the goods and services for which marketing communications may be sent. In this respect, it is not compatible with Art. 13 simply to ask, by a general e-mail, the consent to receive marketing communications[38]

Art. 13 (2) provides an exception to the opt-in regime, which applies for existing customers (restricted opt-out or soft opt-in). This exception is subject to certain conditions: a company, which has obtained its customers' electronic contact details, it can send this person unsolicited messages for purposes of direct marketing of its own similar products and/or services, unless this person has objected to this at the time the contact details had been acquired.This exception, which as such is to be interpreted restrictively, presupposes the lawful collection of contact details and excludes receiving such communications from subsidiaries or mother companies. However, an opt-out possibility should be offered in each marketing message.

Subscribers to a publicly available electronic communications service may be natural or legal persons. The e-privacy Directive is aiming at protecting not only the fundamental rights of natural persons but also the legitimate interests of legal persons.[39] As to the communications to legal persons, member states remain free to determine the appropriate safeguards. However a lot of application difficulties arise: e.g. how the sender can determine that a recipient is a natural or legal person[40]. Another issue pertains to recipients/persons who are users but not subscribers (family members/employees).

2.2.2.1.5 Other legal instruments

In addition the EU institutions have started to include the issue of the fight against spam through international cooperation and other legal texts: The Regulation (EC) No 2006/2004[41] aims at ensuring the cooperation between national authorities responsible for the enforcement

[37] Art. 2 (f) and Recital 17 of the e-Privacy Directive in combination with Art. 2 (h) of the Framework Data Protection Directive.
[38] DPWP, Opinion 5/2004 on unsolicited communications for marketing purposes
[39] Recital 12 of the e-Privacy Directive
[40] Natural persons may use for example mail addresses with pseudonyms or generic terms without being deprived of the protection provided by the Directive.
[41] Regulation (EC) No 2006/2004 of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

of consumer protection laws. The Directive 2005/29/EC concerning unfair business-to-consumer commercial practices protects consumer against such practices, providing inter alia that making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media. is considered to be unfair and misleading (Annex I, 26).[42]

2.2.2.2 Overview of the Legislation in Member States involved to the SPIDER Project

2.2.2.2.1 Bundesrepublik Deutschland

In Germany, the liability question for unsolicited mail containing worms or viruses is still under discussion. However, the German unfair competition law (Gesetz gegen den unlauteren Wettbewerb - UWG, last changed 2004) constitutes that a recipient has to approve the sending of advertisement emails to its own mailbox. However under this law, only a competitor who is dealing with the same activity as the spammer is allowed to file an injunction to the spammer, not the recipient of the spam itself.

Individual persons have the possibility to file an injunction against a Spammer on the basis of the German Common Personal Right (Allgemeines Persönlichkeitsrecht APR) in conjunction with §§ 823 and 1004 of the Civil Law Code (Bürgerliches Gesetzbuch).

The German Government discussed in 2005 an explicit Anti-Spam Law, however it did not pass the discussion phase. A new law (Telemediengesetz) is planned to be passed as bill in 2007, which interdicts in emails deception regarding the actual sender of the mail or commercial interest within the mail.

2.2.2.2.2 Hellas (Greece)

Law 3471/2006 on Protection of personal data and private life in electronic communications sector and amendment of Law 2472/97 (Framework Data Protection Legislation), transposing the e-Privacy Directive.

Law 2251/94 on consumer protection: Article 9 on advertising and Section 2 on unfair terms in consumer contracts may be of particular relevance.

Presidential Decree 131/2003 on certain legal aspects of e-commerce, which transposes EU Directive 2000/31 on e-commerce in the internal market.

2.2.2.2.3 Spain

The laws regulating the sending of unsolicited electronic marketing communications in Spain are the Information Society Services Act 34/2002 and the Telecommunications General Act 32/2003.

Artícle 21.1 of the Information Society Services Act expressly prohibits the sending of advertising or promotional communications by email or other equivalent means of electronic communication which has not been previously requested or expressly authorized by their recipients.

[42] Commission of the European Communities, Communication on Fighting spam, spyware and malicious software, Brussels 15.11.2006, COM (2006) 688 final

The Directive on Privacy in Telecommunications of 12 July 2002 (Directive 58/2002/EC) currently transposed in the Telecommunications General Act 32/2003 which modifies various articles of Act 34/2002 introduced the principle of "opt-in" into the European Union, in other words, prior consent of the person for sending electronic mail having marketing ends.

Both laws grant powers to the Spanish Data Protection Authority. The Telecommunications General Act assigns to the Authority the task of safeguarding the rights and guarantees of subscribers and users in the field of electronic communications, delegating to it the imposition of sanctions for violation in the provision of electronic communication services. On the other hand, the Information Society Services Act sets down that it corresponds to the Authority to impose sanctions in the event of infringement due to the sending of unsolicited marketing communications by electronic mail or equivalent electronic communication means, in breach of the provisions stated in its articles.

In addition to implying an infringement of the Information Society Services Act, the practice of Spam can signify a violation of the right to intimacy and a breach of the legislation on data protection, since it has to be borne in mind that the email address can be considered as personal data.

2.2.2.2.4 Czech Republic

The law 480/2004 ("The law about some services in informational society" from 29.7.2004) regulates the sending of unsolicited electronic marketing communications, spam and allows to send commercial emails after addressees agreement only (principle called "opt-in"). Unsolicited electronic marketing communications are forbidden and senders are punished with a penalty up to 10 millions CZK. The Personal Data Protection Office ("Úřad pro ochranu osobních údajů") fines the penalty.

There is an updating from 20.4.2006. The update distinguishes between current customers and potential customers. According to the update companies are allowed to send commercial emails to theirs current customers without agreements, but these customers can refuse to receive commercial emails at any time. Sending commercial emails to potential customers without prior agreement is considered as unsolicited electronic marketing communications or simply spam.

2.2.2.2.5 Norway

The Marketing Control Act ("Markedsføringsloven") §2b relating to the Control of Marketing and Contract Terms and Conditions prohibits the conduct of businesses to direct marketing at consumers without the prior consent of the recipient. The Marketing Control Act has been revised (in 2005) to accommodate EUs communications directive (2002/58/EF) and applies its lawful base within EU and the European Economic Area (EEA, which Norway is a member of).

Unfortunately, the law neglects to address the SPAM solicitation towards to e-mail addresses of "general nature", thus leaving contact- and non-physical addresses in a grey zone still open to interpretation.

Norway is also taking part in "*London Action Plan on Spam"*.

2.2.3 Spam prevention and detection as potential violation of/interference in fundamental rights

Communication partners may reasonably expect that their communications and their data will not be inspected or recorded by third, public or private parties. However not only the collection/processing of personal data and spam messaging constitutes a threat to privacy.

The fight against spam through the use of filtering techniques arise a lot of questions concerning its compatibility with fundamental rights. Informational and communicational privacy and confidentiality are relevant with regard to preventing spam through filtering. Concerns are expressed in particular of existing practices to inspect communications in order to prevent and eliminate spam. Use of filters and blocking of servers can restrict peoples' ability to communicate and therefore be and impairment of freedom of speech.[43]

2.2.3.1 Right to privacy and confidentiality of communications

Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms provides everyone with the right to respect to his private life and its correspondence. The same Article lays down the conditions under which restrictions of this right could be acceptable, if it is necessary in a democratic society in order to pursue one of the legitimate aims explicitly mentioned in the Convention. Electronic communications are without doubt covered by Art. 8 ECHR, by combining in the most regular cases both the notions of "private life" and "correspondence".[44]

Interception, opening, reading, delaying reception of communications or impeding the sending of letters have been considered to be an intrusion into the right of correspondence, which includes not only confidentiality but also the right to send and receive correspondence. Withholding of received mail constitutes an interference with the provisions of Art. 8.

The confidentiality of communications is guaranteed explicitly by the e-Privacy Directive (Art. 5), prohibiting any form of interception, e.g. a third party acquiring access to the content or traffic data related to private communications between two or more correspondents.[45] Such interceptions are acceptable only on the basis of three fundamental criteria. i.e. legal basis, need for such a measure in a democratic society and conformity with one of the legitimate aims laid down in the Convention: national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others.

For these reasons screening of content through the ISPs and ESPs should considered as intruding fundamental rights and unlawful.

2.2.3.2 Right to personal data – informational self-determination

Blocking spam by technical means without the user's/recipient's consent could intrude on the right to receive and send information, as an expression of informational self-determination.

[43] DPWP, Opinion 2/2006 on privacy issues related to the provision of e-mail screening services (WP 118). Also U. Sury, Datenschutzgerechte Nutzung von Intrusion Detection – Organisatorische und Juristische Implikationen, DuD 29 (2005) 7, pp. 393-398, J. Kabel, Spam: A Terminal Threat to ISP's, Computer und Recht International 2003-1,

[44] DPWP, Opinion 2/2006 on privacy issues related to the provision of e-mail screening services (WP 118).

[45] See also Recitals 3, 21 of the e-Privacy Directive

Filtering tools may not be in compliance with the existing data protection legislation. Subscribers should keep the control over the information concerning them by having "the possibility to opt out of scanning their electronic mails for spam purposes, the possibility to check electronic mails deemed as spam as well as the possibility to decide, what kind of spam should be filtered out"[46].

Another critical point concerns the use of "spam databases". Industry associations and government agencies may collect spam mails[47], which allow tracking user accounts and the users themselves.

2.2.3.3 Freedom of expression

It is quite dangerous to define spam by content. A first risk, related to defining spam by content, concerns freedom of expression/cencorship and breach of communication secrecy. A second risk relates to annoyance by non-commercial messages, which cannot be ignored.[48] However some techniques of communication screening, like blacklisting, can raise questions in relation to the freedom of expression and freedom of information.[49]
Fundamental rights apply also to spammers and their clients. Businesses have the right to advertise their products and, as the European Court of Human Rights has in several cases acknowledged, enjoy freedom of expression. The right to freedom of expression can be restricted with regard to content, e.g. to protect moral and public health or to protect the right of the others, like the right to privacy.
Filtering can also result in the blocking of legitimate information (the so-called false positive), which has as consequence the infringement of the freedom of expression .[IViR]. The DPWP emphasizes that the action of filtering and withholding received mail supposedly unwanted may entail not only an invasion to the freedom of speech but also a violation of freedom of information (Art. 10 of the ECHR) and constitutes an interference of private communications.

2.2.4 Legal grounds and requirements (overview)

The spam issue reflects a conflict between the right to privacy and freedom of expression. European and national legislators have to balance both interests in the process of drawing up national legislation. In this perspective the European Commission invites e-mail service providers to apply a filtering policy, which ensures compliance with the Recommendation of the Data Protection Working Party on e-mail filtering[50]

2.2.4.1 Legal grounds

The collection and processing of data about recipients and spammers as well as the procedures of communications screening as such must be based on legitimate grounds

[46] See Recommendations of the DPWP, Opinion 2/2006 on privacy issues related to the provision of e-mail screening services (WP 118).

[47] Eisentraut mentions the examples the Verband der deutschen Internetwirtschaft e.V, which is collecting spam at hotline@eco.de as well as the Zentrale zur Bekämpfung unlauteren Wettbewerbs, which is collecting spam mails at beschwerestelle@spam.vzbv.de . See P. Eisentraut, Collateral damage – Consequences of Spam and Virus Filtering for the E-mail System

[48] IViR Report

[49] DPWP, Opinion 2/2006 on privacy issues related to the provision of e-mail screening services (WP 118).

[50] Commission of the European Communities, Communication on Fighting spam, spyware and malicious software, Brussels 15.11.2006, COM (2006) 688 final

As to the recipient, data relating to him/her may be processed for the purposes of fighting spam only
a)if the data subject has unambiguously given his/her consent or
b) if processing is deemed to be necessary the performance of a contract to which the data subject is party.[51]
The e-Privacy Directive deals also with the security obligations of the providers (Art. 4 in combination with Art. 16 and 17 of the Framework Data Protection Directive). The DPWP shares the opinion that filtering could be legitimized on the basis that is necessary for the provider to be able to perform properly the service contract to which the data subject, i.e. the recipient is a party. However it is questionable if the obligation to take appropriate technical and organizational measures to safeguard security of data, data systems, services and networks results to a right for subscribers to object to their providers about letting through spam. Providers do have an obligation to act, in the case that access to network or services is impeded due to spam and viruses.[52]
As far as it concerns personal data of the spammers (and to the extent that these data can be considered as personal), the processing could be lawful, if is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[53]The interests of the spammer could not be viewed as overriding the rights of recipients.

2.2.4.2 Data quality

Personal data must be processed fairly and lawfully. They can only be processed for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. The providers must ensure the confidentiality of the filtered communications and that they should not be used for other purposes.
Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. (art. 6)

2.2.4.3 Rights of the Individuals (information, access, correction etc)

If the provider acts as data controller, e.g. he collects and processes personal data for the purposes of spam preventing/filtering he must provide the subscriber/ data subject with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.).In this respective providers should in any case inform their customers about their spam policy and about available technical solutions[54].

[51] Art. 7 of the Framework Data Protection Directive
[52] IViR, 44
[53] Art. 7 e of the Framework Data Protection Directive
[54] An obligation derived from Art. 4 (2) of the e-Privacy Directive.

2.2.4.4 Procedural obligations (Notification)

The controller or his representative, if any, must notify the respective national supervisory data protection authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes, unless an exception from notification is provided by national law.

3 SPIT forms

Before starting describing the SPIT forms, it is worth mentioning that Voice over IP is currently driven by different standards, in particular H.323, Media Gateway Controller Protocol (MGCP) and Session Initiation Protocol (SIP) ([2], [3]). However, the focus in this project will be only on SIP because of its robustness and its growing acceptance by the telecom communities.

SIP is an application-layer protocol for managing multimedia sessions in the Internet. A session can be established between two end-users or more and can involve IP phone calls, conferencing and messaging. SIP is handled through messages such as INVITE for initiating a session and BYE to terminate it. A SIP message may carry a session description that allows media capabilities negotiation between the users. Requests routing in SIP is achieved through proxies, which retrieve the users current location from some SIP registrars designed for this purpose (for more details, we refer to [3]).

As a new emerging IP telephony standard, SIP will certainly be the target of spam attacks. As a consequence, identifying in advance SIP spam and the mechanisms to deal with, is a very crucial task before the problem arises or becomes serious. The different forms of the SIP spam can be categorized as follows,

- *call spam :* this is the case of unsolicited messages for establishing voice or video session. The spammer proceeds to relay his message over the real time media. This form is the usual way used by telemarketers
- *IM spam:* this form is similar to email spam, unsolicited IMs whose content contains the message that the spammer is seeking to convey. The SIP MESSAGE request will be used here but also some other messages such as INVITE with text or html bodies.
- *Presence spam:* Another spam form similar to the IM spam one is called presence spam. The latter is generated by unsolicited presence (subscribe) requests sent to get on the buddy list of a user and then IMs will be sent to this user or some other forms of communications will be initiated.

4 SPIT statistics and prediction

So far, only few SPIT cases are known. These cases were reported (in 2004) by a major Japanese VoIP service provider. A total of 3 cases were detected, but all of them were finally attributed to the same company. Even though these are the only reported SPIT cases, this doesn't mean that these are the only ones that have been produced, but that these SPIT cases might have been very isolated and with no repercussion at all. So, it seems that most of VoIP service providers are still considering that SPIT is not occurring in their VoIP networks or they do not want to disclose the real SPIT statistics in order to reassure their subscribers.

This lack of SPIT statistics can also be explained by the fact that VoIP deployment is still in an infantile stage (the VoIP traffic is currently estimated to be 10% of the PSTN traffic), so there is no not enough VoIP infrastructures deployed to make SPIT profitable for spammers.

In addition, the current VoIP networks can still be considered as islands connected through the PSTN network, and this doesn't make cost effective bulk calls generation.

In spite of the small number of SPIT cases reported, there is no doubt that SPIT will increase in proportion to the deployment of the VoIP network. Traditional PSTN telemarketers will certainly be switching to VoIP at the same time as the PSTN users will be. As a consequence, VoIP will also suffer from the SPIT problem because the objectives of those "spammers" are the same and the techniques can be maintained for both kind of networks. Of course PSTN telemarketers will have to adapt themselves to use VoIP for their activities, but this will surely result in an increase of the number of VoIP undesired calls comparable to the PSTN one if it is not greater. To have an idea of the amount of calls that this may represent, one can check the Federal Communications Commission (FCC)' memo (of 2003) that noted that telemarketers attempted around 104 million calls a day to U.S. businesses consumers.

The case above shows that the number of calls generated by telemarketers can be high, however, this wouldn't be the worst case scenario. That scenario would occur if we consider that the percentage of SPIT calls and Instant Messages (IMs) is going to be as much as SPAM is currently in emails (around 80-85%). In this situation, we should not only consider that customers would be the only ones directly affected by this problem, VoIP service providers would have a serious problem dimensioning their network systems. If that is the case (and this should not be ruled out at all) antiSPIT tools will be indispensable to make VoIP systems usable.

5 SPIT threat analysis

5.1 SPIT identification

5.1.1 Definitions of SIP SPAM vulnerabilities, violations and threats

Spam refers in general to any unsolicited communication [4] and in IP Telephony networks it usually refers to unsolicited bulk calls [5]. In this section, we identify the threats that can lead to SPAM while applying the SIP protocol (RFC 3261).

A **SIP Spam Violation** refers to the transmission of bulk, unsolicited SIP messages of any form. A **SIP Spam Threat** is a possible action or event that exploits a SIP Spam vulnerability to develop a SIP Spam violation. We have identified four possible classes of SIP SPAM vulnerabilities.

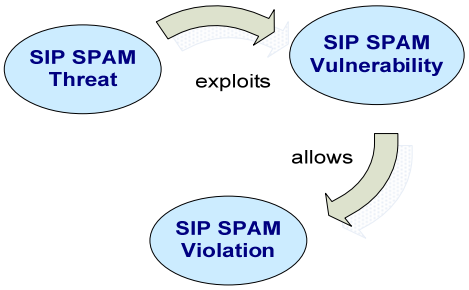

Figure 2:SIP SPAM terms

SIP SPAM vulnerability due to SIP protocol weaknesses

A mandatory characteristic in the description of the structure and functionality of the SIP protocol, that may allow a SIP Spam violation to occur.

SIP SPAM vulnerability due to optional recommendations[55]

A recommendation of the SIP protocol referred to as optional, or not mandatory, that may allow a SIP Spam violation to occur.

SIP SPAM vulnerability due to interoperability with related protocols

A weakness in the specification of other protocols that are used by or interface with SIP (e.g., ARP/DNS/ENUM), that may allow a SIP Spam violation to occur.

SIP SPAM security vulnerability

A weakness in a system allowing an attacker to violate the security (integrity, confidentiality, access control and availability) of the system, or the data and applications it hosts, that may allow a SIP Spam violation to occur.

In the subsequent analysis we provide SIP SPAM vulnerabilities classified to the four aforementioned classes. In the analysis, we identify SIP SPAM threats that refer only to the SIP signaling process, and not on the content of the communication, due to legislative restrictions[56]. In the following the SIP SPAM attacker or spammer is the person, organization or software agent that initiates a SIP Spam Violation.

5.1.2 SIP SPAM vulnerabilities due to SIP protocol weaknesses

S/N	*General Description*	*Detailed Description*
1.1	Listening to a Multicast Address.	SIP specification mentions that Registrations can be sent to the well-known "all SIP servers" multicast address "sip.mcast.net" (224.0.1.75 for IPv4). A spammer listening to that address might become aware of the physical contacts, i.e., locations, of other users.
1.2	Listing of user's Active addresses or locations	The REGISTER message associate a user's URI with the machine's IP address that she/he is currently logged. By exploiting this fact, in conjunction with the vulnerability 1.1, a spammer might discover only "active" addresses, i.e., addresses that are used by online users. This feature enables a spammer to save costs and computational resources, due to the fact that the spam messages will only be sent to online users.

[55] Note that in order to identify the other 3 types of vulnerability, we make the assumption that the RFC3261 has been fully applied, meaning that all the optional recommendations are implemented as mandatory features.
[56] Discussed in section 2.2

1.3	Throwaway SIP accounts	In a SIP environment a user could issue multiple REGISTER messages, thus creating multiple accounts in a domain. A SIP SPAM violation might be based on this option to enable spamming, since it is difficult both the identification of the true originator of the spamming and the usage of e.g., Black Lists.
1.4	Misuse of Stateless Servers.	In the email context, Open Relay Servers are used to forward every message that they receive to its destination. Thus, they become ideal for originating or delivering spamming. They could be exploited by spammers mainly for covering their physical locations or identities, as well as for avoiding spam detection in SMTP headers. According to SIP specifications a SIP stateless proxy offer services that are very similar to an open relay. It forwards every request downstream, and every response upstream. Therefore, it could be exploited for conducting SPIT.
1.5	Anonymous SIP Servers and Back-To-Back User Agents.	A Back-To-Back User Agent (B2BUA) is an entity that acts both as a UAS and a UAC. It also participates in all requests sent on the dialogs it has established. These characteristics make B2BUAs ideal for implementing anonymizing services. B2BUAs and Proxy Servers could become the analogous of Anonymous Re-mailers.
1.6	Sending Messages to Multicast Addresses.	The **Via** header field could contain a parameter with the value "maddr" which corresponds to a destination multicast address. This way a user may initialize spam traffic to a multicast address (multiple recipients) by using the aforementioned parameter.
1.7	Exploitation of Forking Proxies.	A spammer could send an INVITE message containing an ambiguous address to a forking proxy. The forking proxy, after contacting the location service, would send parallel INVITEs to all the addresses returned by the location service.
1.8	Exploitation of Messages and Header Fields Structure.	A spammer could hide the spam message in a SIP message's body, or in other header fields.

		Since the messages bodies and the header fields are rendered by the UA, spam messages are finally delivered to subscribers. The messages and header fields that could be exploited are mentioned below.
1.8.1	Request Methods	Both the INVITE and the ACK request methods could contain a body message. The method MESSAGE could be used to send messages outside of a dialog, where authentication is not mandatory. As a result, the MESSAGE method could result in SIP SPAM violations.
1.8.2	Response Messages	a. **Provisional (1xx) responses** may contain message bodies. b. **180 Ringing** responses could contain a message body. c. **182 Queued** responses may contain a reason phrase or a message body. d. **183 (Session Progress)** may contain a Reason-Phrase or message body. e. **200 OK** responses contain returned information. f. **300 Multiple Choices** responses could include a message body. g. **380 Alternative Service** responses should contain a message body. h. **400 Bad Requests** may contain a Reason-Phrase. i. **480 Temporarily Unavailable** responses could contain a reason phrase. j. **484 Address Incomplete** responses could contain a reason phrase. k. **488 Not Acceptable Here** responses could contain a message body. l. **606 (Not Acceptable)** responses could contain a message body.
1.8.3	Header Fields	a. The **Subject** header field may be displayed to the user. b. The **From** header field allows for a name-text that could be displayed to the user. c. The **Alert-Info** header field specifies an alternative ringback tone (audio file) to the UAC, the spam message in this context. d. The **Call-Info** header field has parameters whose content could be used maliciously.

		e. A **Contact** header field value can contain a display name that may be shown to the subscriber. f. The **To** header field has a "display-name" value, which content can be rendered by a human-user interface. g. The **Retry After** header field may have an optional textual comment. h. The **Error-Info** header field provides a pointer (spam message) to additional information. i. The **Warning** header field may carry text that could be a malicious message. j. The **Content-Disposition** header field describes the way that a message body is to be interpreted by the UA. i. The value "render" denotes that the body should be displayed to the user. ii. The value "icon" denotes that the body is an image that should be displayed to the user (spam message). k. The **Content-Type** header field denotes the media type of the message body delivered to the user. The spammer could place the spam message on the body and deliver it to the subscriber. Additionally, these header fields could lead a UA into executing the message body (that could be a spam virus). l. The **Priority** header field signifies the urgency of the request. Using a high priority value the spammer could send messages with higher probabilities of being received.

5.1.3 SIP SPAM vulnerabilities due to optional recommendations

S/N	*General Description*	*Detailed Description*
2.1	Sending Ambiguous Requests to Proxies.	If the **Request-URI** send by the user does not provide sufficient information for the proxy to determine the target set, it might return a **485 Ambiguous** response message. These responses could contain a **Contact** header field with a list of possible new addresses to be tried. A spammer could send a URI

		"a@example.com" and the server might return all the names starting from "a", thus resulting in the population of users list.
2.2	Contacting a Redirect Server with Ambiguous Requests.	When a Redirect Server receives a request other than CANCEL, it either refuses the request or gathers the list of alternative locations from the location service and returns them. A SIP SPAM violation might occur when a dictionary attack to a redirect server is used, which, after consulting a location service, it will return alternatives locations, thus allowing the population of users lists.
2.3	Exploitation of Registrars Servers	A Registrar Server acts as the front end to the location service for a domain. Thus, it can query the location service for specific registrations. A SIP SPAM violation might occur when one of the attacks mentioned previously (i.e., a dictionary attack, a query with special characters, etc.) is initiated to a Registrar, acquiring lists of names.

5.1.4 SIP SPAM vulnerabilites due to interoperability with related protocols

S/N	*General Description*	*Detailed Description*
3.1	SPIT due to DNS vulnerabilities	In the context of ENUM, passing off could occur when an entity enters at DNS its own details in the NAPTR records that corresponds to another person's number. Passing off weakens the trust that individuals and organizations should have in transactions. As an effect, a spammer can populate DNS with false data and create SPIT Calls.
3.2	ENUM Registration Vulnerability may be subject to influence SPIT Calls	The ENUM registrant interacts with various entities to provide ENUM records. The registrant must request registration through an accredited registrar, who authenticate the registrant and validates his number assignment. Depending on the registrant's selection, the registrant can populate registry with new NAPTR records. Cache poisoning of the NAPTR record may be populated across the hierarchical structure of ENUM servers.

3.3	ENUM may influence the reception of the called party contact methods	In the ENUM calling party control approach, the use initiating the call may receive all the contact info (e.g. PSTN number, SIP E.164 address, email). This may create various type of spam (e.g. email spam, SPIT towards both VoIP and PSTN networks etc)
3.4	Public ENUM versus Private ENUM	Private ENUM can be used by carriers found to interconnect their VoIP islands. Private is basely used to support LNP and its records may be different from public ENUM. In addition, a carrier ENUM could undermine end-users privacy as it can be possible for others to identify "ex-directory" or unpublished numbers based on their ENUM registration. This has the same impact as 3.3
3.5	Anonymity	ENUM could generate anonymity (e.g. user's credentials) may not be transmitted towards the called party, giving the opportunity to spammers to generate SPIT calls. This may be applied in the case when private ENUM may be used to interconnect VoIP islands.

5.1.5 SIP SPAM security vulnerabilities

S/N	*General Description*	*Detailed Description*
4.1	Observing Traffic near SIP Servers	A spammer with the ability to capture packets on a communication channel near a Registrar or a Proxy, could extract the **To**, **Via** and **Contact** header fields from SIP messages and create a list of possible spam messages recipients.
4.2	Port Scanning the Well-Known SIP Ports	SIP UAs use the well-known ports 5060 and 5061 for SIP communications. The spammer may launch a Port-Scanning attack, and record all the addresses that listen to these ports. This way the malicious user may populate a user list.
4.3	Proxy-In-The-Middle	SIP specification defines strong security mechanisms for the intra-communication of proxies, such as authentication, TLS and IPSEC. However, due to the fact that SIP proxies operate in the internet environment, they are prone to a wide variety of attacks.

		These could result in the hijacking of a SIP proxy by an attacker, despite using strong security for protecting SIP communications. A Proxy-In-The-Middle attack could put the whole communication model at risk.
4.4	Exploitation of Re-INVITES Request Messages	Re-INVITES can modify both the dialog and the session's parameters (e.g. add media streams to dialogues). A Proxy-in-the-Middle could send spoofed re-INVITES (to both ends of communication) adding media streams that contain a spam message.
4.5	Exploitation of the Record-Route Header Field	Using the **Record-Route** header field, a Proxy server can remain in the SIP messaging path beyond the initial INVITE. This characteristic enables the implementation of various mid-call features. A malicious proxy might use these mid-calls features, for delivering spam messages.

5.2 VoIP potential spammers

The motivation of Spammers are so simple as convincing, it is all about money. The costs of spamming in a E-mail or SIP Environment are that low that a spammer can reach thousands of millions of potential customers every day. To be cost effective, the feedback rate for a Spam wave do not need to be very high. For E-mail, one can note the existing of a lot of calculation examples[57] what a Spam wave costs and how much a Spammer approxamitly gain from it. We can suppose that the SPIT revenue model is only slightly different. A very rough example helps to understand the potential of SPIT for a Spammer:

- A Spammer advertise a product which costs himself round about 20€ inclusive shipping to his customers
- He sells the product for 40€
- 10€ he has to pay to send 10.000 SPITs, which is a obvious high price
- Every 10.000th SPIT finds a customer, this is a guessed but reasonable value
- The Spammer sends 1.000.000 SPITs / day
- So he finds 100 customers per day
- This results in an earing of 1000€ each day

The calculation for a day:

Product costs	-20 €	
Sending costs	-10 €	
Selling price	40 €	
Total / customer	10 €	* 100 customer = **1000€ / day**

[57] Nov 2006, Spam economy: http://rejo.zenger.nl/abuse/1085493870.php

The values of this example are only predicted, but they are all reasonable. In the real world they will be different but it helps to understand an important thing: spamming is profitable. Even if a Spammer earns only 100€ per day that is still an income of over 3000€ per month. That is the major reason why spamming never disappears in the E-mail environment and will appear in the SIP environment.

5.2.1 SPAM Infrastructure

The infrastructure for distributing Spams has constantly changed over the last years. In the beginning the Spammers used their own dedicated computers. To increase their output and to avoid the blocking by ISPs they increased the amount of servers and connections to the Internet. It is not uncommon that some Spammers have several server farms with more than one hundred servers. With such a huge amount of servers they have the ability to send millions of Spams.

Every day where a Spammer can not send E-mails, Instant Messages or issue phone calls means to him a day without any income, so he tries to avoid this situation. The server farms are connected to several ISPs so even if an ISP disconnects a connection they can still continue with their business while they search for an other ISP.

The situation for Spammers became harder for Spammers in the last years with the start of, so called, RBLs (Realtime Black Lists). These RBLs try to collect and provide informations about IP Adresses which are used by Spammers. This information can be used to block any connections from the known Spam IP Adresses. This type of Spam protection was effective for some time until the Spammers has changed their methods again.

Today the Spammers are using so called Bot-Networks. These networks consist of computers which are infected or captured by computer viruses, spy or malware. These computers run a piece of software which is controlled by a Spammer and will be used to distribute Spams. The software will run in the background, hidden from the original owner of the dedicated computer. So an infected computer will be part of a Botnet until the owner of the computer will remove this type of Software, this is not an easy job. So the amount of computers in such Botnetworks increases rapidly. Today the number of Botnet computers is increasing by 250.000 to 500.000 computers each day. The Spammer can change the software as often as he want. And they do it. It is a cat and mouse game. Every time a Spam technique is blocked by the Anti Spam vendors, the spammers try to improve this technique or to build up a new one. The goal is always reaching as much as possible potential customers that are supposed to buy their products. It is only a matter of time until the Spammers tries to reach new customers with the VoIP technology. They have the infrastructure and they will be able to modify their Botnet software so that this software can distribute their advertisings as SPIT.

5.3 VoIP spammers capabilities

In this section, we describe the possible ways of generating SPIT and we identify the different issues that the potential VoIP spammers will face. We also describe the available tools, which seem to be suitable for SPIT generation as well as the ways of using them.

SPIT generation problematic can be splited into three parts:

1. Obtaining list of target addresses (SIP URI)
2. Getting connection to the VoIP networks
3. The generation of SPIT call and Instant Messaging

5.3.1 URIs mining

Before a spammer can start generating spam calls, he needs to get the list of SIP URIs of his future victims. The easy way to get these lists seems to be the misuse of the ENUM service. ENUM service stores huge amount of SIP URIs that can be very easily obtained.

Example of simple BASH script for mining of URIs from ENUM:

```
prefix=5.4.7.2.2.2.0.2.4.e164.arpa
for (( i=120 ; i<=999; i++ )) ; do
    num=$((i % 10)).$((($i / 10) % 10)).$((($i / 100) % 10))
    fullnum=$num.$prefix
    echo $fullnum
    dig -t naptr +short $fullnum
done
```

Another possibility can be the usage of classical methods known from E-mail spamming like robots for getting E-mail addresses from web pages. Fortunately, it is not so widely common today to use SIP contacts on web pages especially in registration forms, in conferences, etc. So such type of URIs harvesting is very limited today.

5.3.2 Getting VoIP connectivity

Once we have collected users SIP URIs, the simplest way to contact these users is to send INVITE messages to the SIP proxies that serve these users domains. This lookup can be done easily by usage of DNS (preferably SRV records, if the proxy for requested domain is in the DNS). Furthermore, this lookup can be done by User Agents or by SIP proxies (these proxies can be private or public but misused in this case).

Another possibility is to send the INVITE messages directly to end phones without cooperation with proxies for the served domain. By this, we can pass through some SPIT filters implemented on SIP proxy. The location of the targeted SIP phones have to be obtained from earlier communication where we can initiate call with usage of SIP proxies for user's domain and for example from the Contact header of 180 RINGING response we can get the IP address of the targeted phone. This method has great number of restrictions. For example there can be a firewall in the target network filtering communication on SIP (RTP) ports from other nodes than SIP proxy (RTP proxy), the address where the phone is listening could vary in time (is reregistered on SIP proxy), responses are going still through the SIP proxy etc.

5.3.3 SPIT call generation

It this paragraph, we provide an overview of some interesting free tools that could be easily used for spit calls generation. For the latter, some software able to generate calls including

both SIP and RTP flows are needed. Also the possibility to freely define various call parameters such as targeted IP and targeted URI is required.

The following tools have been recognized as suitable for SPIT calls generation:

SIPp

SIPp is a free Open Source test tool and traffic generator for the SIP protocol. It includes a few basic SipStone user agent scenarios (UAC and UAS) and establishes and releases multiple calls with the INVITE and BYE methods. It can also reads custom XML scenario files describing from very simple to complex call flows. It features the dynamic display of statistics about running tests (call rate, round trip delay, and message statistics), periodic CSV statistics dumps, TCP and UDP over multiple sockets or multiplexed with retransmission management and dynamically adjustable call rates. SIPp can also send media (RTP) traffic through RTP echo and RTP / pcap replay. Media can be audio or audio and video.

Following, is an example describing a part of an XML scenario file for generating SPIT calls including desired RTP message (text of SIP messages was removed because of simplicity):

```
<scenario name="UAC with media">
  <send retrans="5">
    <![CDATA[
INVITE MESSAGE TEXT
    ]]>
  </send>

  <recv response="100" optional="true">  </recv>
  <recv response="180" optional="true">  </recv>
  <recv response="200" rtd="true" crlf="true">  </recv>

  <send>
    <![CDATA[
ACK MESSAGE TEXT
    ]]>
  </send>

  <!-- Play a pre-recorded PCAP file (RTP stream)                    -->
  <nop>
    <action>
      <exec play_pcap_audio="pcap/SOME_PRERECORDED_MESSAGE.pcap"/>
    </action>
  </nop>

  <pause milliseconds="8000"/>

 <send retrans="500">
    <![CDATA[
BYE MESSAGE TEXT
    ]]>
  </send>

  <recv response="200" crlf="true">  </recv>

</scenario>
```

PJSIP

For the case of building own SPIT generation tools the PJSIP framework can be used. It support both SIP and media generation and is designed as multiplatform solution.

5.4 SPIT threat assessment

The threat assessment is conducted according to the methodology described in Table 1. In our evaluation, three criteria are considered: *Likelihood* and *Impact*. The *Likelihood* evaluates the possibility that SPIT activities related to a given threat are conducted. The technical difficulties that a spammer has to resolve are the main factor defining the Likelihood. The latter is *low* if the spammer has to resolve strong technical difficulties. The Likelihood is *possible* if there are technical difficulties but solvable. The Likelihood is *likely* if there are no technical difficulties that need to be solved to mount a SPIT activity. The Impact criterion evaluates the consequences of a SPIT activity related to a given threat. The Impact is *low* if a SPIT activity creates only annoyance to the user. In this case, the consequences can be repaired. The Impact is *medium* if the SPIT activity is directed to a single user and the latter will experience a loss of productivity for a considerable mount of time. The Impact is *high* if a SPIT activity is directed to a huge number of users and causes a large-scale loss of productivity. The scale that has been used to assign values to the Likelihood and Impact is Low (1), Medium (3) and High (5).

Criteria	Cases	Difficulty	Rank
Likelihood	Unlikely (Low)	Strong	1
	Possible (Medium)	Solvable	3
	Likely (High)	None	5
Impact	Low	Annoyance	1
	Medium	Loss of productivity	3
	High	Large scale loss of productivity	5
Risk	Minor (Low)	No need for countermeasures	1,4
	Major (Medium)	Threat needs to be handled	4,16
	Critical (High)	High priority	16,25

Table 1: Risk evaluation methodology

In order to assess the risk regarding the recognized SIP's threats we consider both the commercial and the technical points of view. In other words, The VoIP providers within the SPIDER consortium (i.e VozTelecom and Telio) have evaluated the threats listed in section 5.1 according to the impact of the corresponding attacks on their companies business. These threats were also evaluated technically according to the methodology discussed above. To take benefit from both evaluations, a merging was achieved according to the following formulas,

$L = a*Li + A* Lj$, regarding the Likelihood, and
$I = A*Ii + a*Ij$, regarding the Impact,

The *Li, Ii* indicate the assessment values assigned by the VoIP providers, however the *Lj, Ij* indicate the technical evaluation. Additionally, *A,* and *a* indicate the weights given to each assessment. We choose the values of *A* and *a* to be 0,6 and 0,4, respectively, so as the assessments of the VoIP providers to be more important regarding the *Impact* and the technical assessment to be more important regarding the *Likelihood*. For a given threat, the ***Risk*** is defined as the product of the Likelihood and the Impact values. The computation of the Risk was based on the formula $R = L * I$ and the scale that has been used is Low if *R belongs to the interval [1,4]*, Medium if *R belongs to (4,16]* and High if *R belongs to (16,25]*. In the case where there was no impact from the service provider, we set *Li=0, Ii=0* and *A=a=1.*

5.4.1 SIP SPAM vulnerabilities due to SIP protocol weaknesses

In this section, we evaluate, based on the methodology defined earlier, the threats related to the SIP protocol weaknesses.

Threat #	Description	Provider Answer		Technical Answers		Merged		
		Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Risk
1.1	Listening to a Multicast Address.	Low (1)	Medium (3)	High (5)	High (5)	Medium (3.4)	Medium (3.8)	Medium (13)
1.2	Listing of user's Active addresses or locations	Low (1)	Low (1)	High (5)	Low (1)	Medium (3.4)	Low (1)	Low (3.4)
1.3	Throwaway SIP accounts	Low (1)	Low (1)	High (5)	High (5)	Medium (3.4)	Medium (2.6)	Medium (8.8)
1.4	Misuse of Stateless Servers	High (5)	High (5)	Low (1)	High (5)	Medium (2.6)	High (5)	Medium (13)
1.5	Anonymous SIP Servers and Back-To-Back User Agents	High (5)	Medium (3)	Low (1)	Medium (3)	Medium (2.6)	Medium (3)	Medium (7.8)
1.6	Sending Messages to Multicast Addresses.	Low (1)	Low (1)	High (5)	High (5)	Medium (3.4)	Medium (2.6)	Medium (8.8)

Threat #	Description	Provider Answer		Technical Answers		Merged		
		Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Risk
1.7	Exploitation of Forking Proxies.	Low (1)	Medium (3)	High (5)	High (5)	Medium (3.4)	Medium (3.8)	Medium (12.9)
1.8.1	Request Methods (Invite and ACK)	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (6.1)
1.8.1	Request Methods (Message)	Medium (3)	Medium (3)	High (5)	Medium (3)	High (4.2)	Medium (3)	Medium (12.6)
1.8.2	Resp. Messages: 180, 182 and 183	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.2	Resp. Message: 200 OK	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.2	Resp. Messages: 300, and 380	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.2	Resp. Messages: 400, 480, 484, and 488	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.2	Resp. Message: 606 Not Acceptable	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Fields Subject From, Contact, To	Medium (3)	Low (1)	High (5)	Medium (3)	High (4.2)	Low (1.8)	Medium (7.5)
1.8.3	Header Fields Alert-Info	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Fields Call-Info	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Retry After	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Error-Info	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Warning	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Content-Disposition	Low (1)	Low (1)	High (5)	Medium (3)	Medium (3.4)	Low (1.8)	Medium (8.8)
1.8.3	Header Content-Type	Medium (3)	Medium (3)	High (5)	Medium (3)	High (4.2)	Medium (3)	Medium (12.6)
1.8.3	Misuse of Priority Header	Medium (3)	Medium (3)	High (5)	Medium (3)	High (4.2)	Medium (3)	Medium (12.6)

Table 2: SIP protocol weaknesses evaluation

5.4.2 SIP SPAM vulnerabilities due to optional recommendations

Here, threats related to SIP optional recommendations are evaluated according to the methodology described earlier.

Threat #	Description	Provider Answer		Technical Answers		Merged		
		Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Risk
2.1	Sending Ambiguous Requests to Proxies	-	-	High (3)	High (3)	High (5)	High (5)	High (25)
2.2	Contacting a Redirect Server with Ambiguous Requests	-	-	High (3)	High (3)	High (5)	High (5)	High (25)
2.3	Exploitation of Registrars Servers	-	-	High (3)	High (3)	High (5)	High (5)	High (25)

Table 3: SIP optional recommendations threats evaluation

5.1.4 SIP SPAM vulnerabilities due to interoperability with related protocols

In this section, we evaluate the SPIT vulnerabilities due to the interoperability of SIP with other protocols.

Threat #	Description	Provider Answer		Technical Answers		Merged		
		Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Risk
3.1	SPIT due to DNS vulnerabilities	-	-	High (3)	High (3)	High (5)	High (5)	High (25)
3.2	ENUM Registration Vulnerability	-	-	High (3)	High (3)	High (5)	High (5)	High (25)
3.3	ENUM may influence the reception of the called party contact methods	-	-	High (3)	High (3)	High (5)	High (5)	High (25)
3.4	Public ENUM versus Private ENUM	-	-	High (3)	High (3)	High (5)	High (5)	High (25)
3.5	Anonymity	-	-	High (3)	High (3)	High (5)	High (5)	High (25)

Table 4:SIP interoperability threats evaluation

5.4.4 SIP SPAM security vulnerabilities

Here the threats related to SIP security vulnerabilities are assessed.

Threat #	Description	Provider Answer		Technical Answers		Merged		
		Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Risk
4.1	Observing Traffic near SIP Servers	Low (1)	Low (1)	Low (1)	High (5)	Low (1)	Low (3.8)	Low (3.8)
4.2	Port Scanning the Well-Known SIP Ports	High (5)	Low (1)	High (5)	High (5)	High (5)	Medium (2.6)	Medium (13)
4.4	Exploitation of Re-INVITES Request Messages	Low (1)	High (5)	Low (1)	High (5)	Low (1)	High (5)	Medium (5)
4.5	Exploitation of the Record-Route Header Field	Low (1)	High (5)	Low (1)	High (5)	Low (1)	High (5)	Medium (5)

Table 5:SIP security vulnerabilities evaluation

6 Conclusion

SIP based Voice over IP (VoIP) is an emerging technology that will certainly suffer from the SPAM problem in the future. In this deliverable, we tried to better understand the SIP SPAM problem in order to define the adequate mechanisms for protecting the SIP infrastructures. In fact, we have focused on providing accurate and useful information about prior SIP SPAM activities that could help prevent some future ones from occurring.

We started this document by discussing the SPAM terminology from both technical and legal points of view. Moreover, we brought to light on the one side the motivations behind carrying out this kind of activities and on the other side the tools that make the spammers capable of achieving their goals.

One of the key findings of this study is the identification of the SIP protocol vulnerabilities that can be used by the spammers to generate SPAM “attacks”. By addressing these vulnerabilities in details, it may be possible to mitigate the SIP SPAM activities. This inspection process, known as SPIT threat assessment, takes these findings one step further by identifying the eventual SPIT scenarios and evaluating them in order to put a first stone in building appropriate techniques that can help in the SPIT fighting operation.

7 References

[1] Dealing Effectively with Spam, link : http://www.secinf.net/anti_spam/Dealing_Effectively_with_Spam_.html

[2] J. Rosenberg et al, "SIP: Session Initiation Protocol", RFC 3261, June 2002

[3] J. Rosenberg et al, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002

[4] Y. Rebahi, and D. Sisalem, "SIP *Service Providers and the Spam Problem*", in Proc. of Voice over IP Security Workshop, Jun. 2005.

[5] R. MacIntosh, and D. Vinokurov, "*Detection and mitigation of spam in IP telephony networks using signaling protocol analysis*", in Proc. of 2005 IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, Apr. 2005.

[6] A. Johnston, "*Understanding the Session Initiation Protocol*", 2nd Edition, Artech House, 2004.

[7] J. Rosenberg, J. Peterson, and C. Jennings, "*The Session Initiation Protocol (SIP) and Spam*", Internet Draft, October 2006.

[8] R. Kuhn, T. Walsh, and S. Fries, "*Security Considerations for Voice Over IP Systems*", Recommendations of the National Institute of Standards and Technology, NIST SP 800-58, 2005

[9] D. Endler et al., "*VoIP Security and Privacy Threat Taxonomy*", Voice over IP Security Alliance (VOIPSA), 2005.

[10] ITU ENUM Page, available at http://www.itu.int/osg/spu/enum/index.html

[11] G. Kambourakis, D. Geneiatakis, S. Gritzalis, T. Dagiuklas and C. Lambrinoudakis, "*Security and Privacy Issues towards ENUM protocol*", 12th IEEE ISSPIT, Athens, Greece, December 2005.

[12] P. Faltstrom, "*E.164 number and DNS*", RFC 2916, September 2000

[13] R. Brandner, "*IANA Registration for Enumservice Voice*", RFC 4415, February 2006

[14] R. Brandner, "IANA Registration for Enumservices email, fax, mms, ems, and sms", RFC 4355, January 2006