

# Dealing with Spam in Voice Over IP

Nilton Bila

nilton@cs.toronto.edu

Department of Computer Science

University of Toronto

**ABSTRACT.** *Voice over IP is emerging as the new standard in telephony. It inexpensively routes calls worldwide and consumers are embracing it. Inexpensive communications opens the door for unsolicited calls. In this paper we investigate spam in VoIP, discuss properties of the technology that make it vulnerable to spam and propose the use of techniques which impose cost to spammers as an effective approach to fighting spam.*

## 1 INTRODUCTION

Voice over the Internet Protocol (VoIP) is a growing technology. Major Internet Service Providers not traditionally associated with telephony now provide various VoIP offerings. For example, AOL offers TotalTalk [1], EarthLink offers trueVoice [15], Comcast offers Digital Voice [10] and Rogers offers Internet Phone [32]. VoIP is enabling even providers with no network infrastructure, such as AOL, to compete in the telephony market. At present, VoIP solutions are marketed in two flavours: as computer based internet services employing software clients such as Skype, or as home phone "lines" aimed at replacing the traditional telephony and employ hardware client devices such as analogue phones. Skype [36] is an example of the former whereas Vonage [39], EarthLink, Rogers and Comcast's offerings are examples of the latter flavour.

Consumers are embracing IP telephony as it offers savings when compared to traditional Public Switched Telephone Network (PSTN) telephone service. For households, VoIP offers inexpensive long distance in two forms. First, by allowing the transmission of voice traffic over the existing networks, calls can be made to virtually any city as if they were local, as long as the provider has a PSTN gateway in the destination city. Secondly, users are able to choose numbers in arbitrary local areas, enabling persons in those local areas to call them at local rates. Moreover VoIP providers often bill calls based on the local area chosen

by the customer and not the physical location of their telephone device. The fact that long distance calls are cheaper with VoIP can be seen, for example, from EarthLink telephone service plan which bundles unlimited free long distance calling to the U.S. and Canada, all at a monthly rate of \$24.95, something unseen in traditional telephony.

For corporations, in addition to the benefits gained from inexpensive long distance calling, VoIP allows them to integrate their data and voice networks simplifying their management and enabling further savings. It also allows corporations to integrate branches in multiple locations through free voice communication between them. As such, the Federal Communications Commission projects that 19% of U.S. firms will use VoIP by next year [28].

The number of VoIP users is growing every day. Skype, for example, services over 99 million users worldwide as of April 2006 [36]. Vonage, a home phone VoIP service providers boasts over 1.5 million active subscribers [39].

However, inexpensive telecommunication makes broadcasting to masses affordable to anyone, and this has been known to be abused for commercial interests. E-mail is today cluttered with unsolicited messages known as spam. As of early 2004, over 50% of e-mail messages sent worldwide were spam [18]. Likewise, free local telephone calls have been known to be exploited by telemarketers who make use of automated dialers. VoIP extends the concept of local calling to potentially include subscribers world wide. Moreover, as we later show, addressing in VoIP is no different than in the e-mail or traditional telephone systems, therefore allowing VoIP spammers to harvest addresses using the same techniques they already employ in the older media.

Unsolicited calls in VoIP are known as SPIT, SPam over Internet Telephony. We consider SPIT to include all calls which are unsolicited, unwanted and irrelevant to the called party, whether pre-

recorded messages or calls made by human callers.

The motivation for this work is thus the need to understand the present state of SPIT, the potential for its growth as VoIP gains critical mass of use, and recommend effective techniques to curb SPIT. We believe that it is essential to develop and implement these techniques before VoIP becomes widely used to avoid costs of changing the VoIP infrastructure and protocols after its wide adoption. It is better to implement SPIT containment features now because experience from the IP protocol has shown that proposals to modify widely established protocols and infrastructure are likely to fail because of strong resistance to change [34, 4, 37].

Interest in spam over Internet telephony is only recently awakening, fuelled by dependability and security concerns. For example, a grant has been recently awarded by the National Science Foundation (NSF) to researchers at the University of North Texas to investigate spam in VoIP as well as security vulnerabilities.

From this work, we report that SPIT is not yet a problem in VoIP networks, we identify weaknesses of the VoIP medium in dealing with SPIT and recommend techniques that provide deterrent for VoIP spammers.

The remainder of the paper is organized as follows. In the next section we provide an overview of VoIP implementations. In Section 3 we discuss the methodology employed in our study of SPIT. In 4 we discuss the findings from the study. In Section 5 we make recommendations on effective strategies for curbing SPIT, and follow up in 6 with a discussion of work that relate to ours. In Section 7 we discuss avenues for future work and conclude in 8.

## 2 BACKGROUND

At present, there are many implementations of VoIP, some employing open protocols, others employing closed and proprietary ones. Virtually all implementations employ a signalling protocol for control and establishment of calls and a streaming protocol for multimedia exchange. Little is known about the protocols of proprietary VoIP networks such as Skype. The little information is attained either by reverse engineering the clients such as in [6] or by monitoring network traffic of clients such as in [20, 2].

The Session Initiation Protocol (SIP) [33] together with Real Time Protocol (RTP) [35] are the dominant open protocols employed in VoIP for signalling and media streaming, respectively. Although SIP supports a variety of real-time streaming protocols, it is often used with RTP and the two are collectively referred to as SIP voice over IP telephony. SIP is an IETF Internet standard track protocol which comprises two primary entities: user agents and proxies. A user agent acts as both a client, when it initiates calls to other agents, and a server, when it responds to calls. Proxies forward signalling messages between user agents and provide permanent addresses to clients even if client is mobile, in similarity to a home agent in Mobile IP [27]. RTP is an IETF Internet standard protocol for transport of real time data including audio and video.

In figures 1(a) through 1(c) we summarize the steps employed in establishing a SIP call. In the figures, we present two SIP providers, represented by their respective domains toronto.edu and sip-r-us.com, each having a proxy server and one user. In 1(a) user bob@toronto.edu initiates a call by sending an invitation message to joe@sip-r-us.com. The invitation is sent first to the user's own proxy (toronto.edu) which forwards it to the proxy at sip-r-us.com. The sip-r-us.com proxy, knowing Joe's actual address, forwards the request to Joe's user agent. Upon receiving the INVITE request, Joe's agent will provide a notification of incoming call to Joe, such as by means of an audible ring tone. When Joe answers the call a "200 OK" message is issued in the reverse direction notifying Bob that Joe has accepted the call. Once the call is established, RTP streams are set up between the user's agents which transmit voice data in both directions. The media streams bridge a direct link between the two call parties and do not make use of proxies.

We should note from figure 1 that addressing in SIP resembles e-mail addressing whereby a contact is formatted as a user name at a particular domain. We discuss the implications of this addressing for SPIT in Section 4. This form of addressing is, however, not suitable for analogue telephone devices, as these are designed for numeric addresses. In 1(d) we show how support for analogue devices is provided. Analogue Telephone Adapters (ATA) are employed at the end points to bridge a link between the Internet

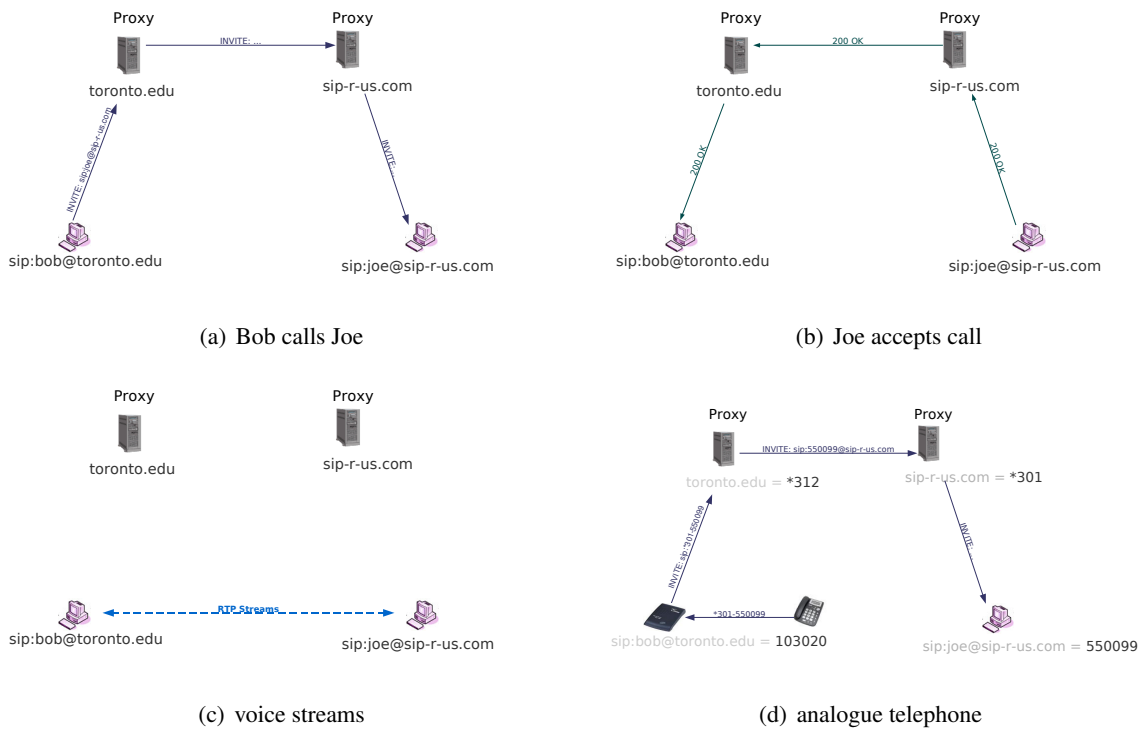


Figure 1. Overview of a SIP call. Figures 1(a) through 1(c) show the establishment of a call. Figure 1(d) shows how analogue telephones are supported through translation of SIP addresses.

and analogue devices. ATAs translate call initiation from a sequence of numbers into SIP requests, convert audio streams into analogue sound and vice-versa, as well, they provide signals to analogue devices.

Figure 1 also shows how proxies are used to facilitate calls. However, as we discuss in Section 3 calls can be made without the intervention of a proxy at either end. Knowing the host address and port at which an agent listens for calls, anyone can dial there directly, as we validated. Moreover, calls are not restricted to SIP end-points only. Service providers often employ PSTN gateways at the proxy level which accept SIP calls from within the network and forward to PSTN telephones be it land lines or cellular phones. These gateways also accept calls from PSTN phones and forward to SIP addresses.

Although our work centers on SIP, we also look at the Skype network to gain an understanding of the nature of SPIT as VoIP networks grow. The SIP networks we looked boast an average of only 500,000 users which we found not to provide the critical mass for the presence of full-fledged SPIT activity. Skype boasts, in comparison near 100,000,000 users. Skype is a peer-to-peer

VoIP network in which clients maintain a set of neighbours and use these to locate other users in the overlay. This model does not employ proxies as is case with SIP, although peers with good internet connections can serve as super peers which relay traffic between underprovisioned or firewalled peers.

### 3 METHODOLOGY

We developed a set of experiments to provide an understanding of the state of SPIT in existing VoIP networks and identify properties of these networks which impact their vulnerability to SPIT. We describe below the set of experiments conducted.

#### 3.1 Answering Machine Experiments

These experiments consist of instantiating publically accessible VoIP clients to act as answering machines. This is a passive approach to SPIT detection which resembles honey pots and was conducted in both SIP and Skype networks.

The objectives of these experiments were to understand how much SPIT exists in these VoIP networks and what characteristics SPIT presents. Characteristics we were interested in include the average length of calls, whether automation is

employed SPITters, the bandwidth requirements of messages, their content, how SPIT scales with the number of users, among others.

We detail next the set up of the experiments.

### 3.1.1 SIP

For this experiment, we made modifications to Shtoom [3], a SIP client, to accept and record multiple calls and repackaged it in a self contained archive from which it can be executed on most Linux hosts without requiring root privileges for installation. Shtoom is a Python based application which requires the availability of Python libraries such as the Zope Interface [14] and Twisted [23] within Python's root installation directories. We needed to build self contained packages to allow us to deploy multiple clients within hosts we could have online 24 hours a day.

We set up 9 clients online with an equal number of accounts at 3 different SIP providers for a period of 47 days. We published their addresses at searchable user directories of the providers, and for three of the accounts, posted their addresses on a web page which has been indexed by search engines such as Google, Yahoo and Altavista. The SIP providers in use have together in excess of one million users. Our eventual goal was to set up more clients, however, from our preliminary findings we do not judge this necessary as we find that SPIT is not yet characteristic in these networks.

On the same host in which the clients executed, using Ethereal [16] network packet analyser, we captured all network packets exchanged with the clients during calls.

### 3.1.2 Skype

Although the use of Skype in these experiments was similar in spirit to that of SIP, we were unable to make modifications to the Skype client due to its proprietary nature. Instead we made use of existing features of the Linux version of the client and interposed a Linux library for audio capturing. For this experiment we made use of version 1.2.0.18, which provides the ability to automatically accept incoming calls and maintains a log of received calls. To be able to record calls, we interposed the vsound library which captures the client's output to the sound device and records it to disk.

We run two Skype clients for a period of 14 days. We also made use of the Ethereal packet analyser to gain an understanding of the network usage during calls.

## 3.2 Ad-Hoc Experiments

To understand protocol and implementation properties such as whether it is possible to make calls without employing proxies, whether free calls to PSTN telephone lines are possible from SIP accounts, how SIP providers are addressing SPIT, we experimented with existing networks.

We made calls by employing proxies, no proxy, and a proxy at either side of the call and were successful in all cases. We learnt that a number of institutions such as universities make peering arrangements with SIP providers which allow SIP users to dial landlines at those institutions free of charge. We successfully tested by making calls to arbitrary numbers at universities.

To facilitate the use of analogue telephone devices with SIP, as shown in figure 1(d) providers assign numeric addresses to users. We found by signing up for accounts at different times that the numbering is sequential, therefore simplifying a SPITter's task of guessing numbers.

## 3.3 Validation of Techniques

We were intent on validating different techniques to curb spam by running simulations on traces of SIP users. Our first approach was to monitor users' status by probing their agents periodically on whether they are online, offline or on call. However, we encountered several problems with this approach. Among others, obtaining user status by sending call initiation requests is not sustainable as these requests are intrusive. This form of monitoring would not work well as we found that providers offer free voice mail resulting in this technique always reporting that users are online. Moreover, the information obtained from this form of monitoring would not allow us to determine if users accept calls from individuals not listed in their contacts. The soft clients employed in the SIP networks we tested allow users to maintain a list of contacts and know when they are online, provided that they were granted authorization by the contact. Accepting and engaging in calls from non-buddies implies that techniques such as whitelisting calls cannot be used to fight SPIT.

In our second approach, we contacted administrators at two SIP service providers and requested anonymized user logs. We received an affirmative response to one of our requests, however, two weeks later we have had no

success in obtaining the logs. Throughout this contact with the administrators, we have also conducted informal interviews by e-mail and instant messaging to get a sense of the experiences with SPIT these providers have had. We discuss our findings in the next section.

## **4 FINDINGS**

We first discuss properties of protocols and implementations of VoIP which impact VoIP's vulnerability to SPIT. In the subsequent subsections we look at the calls received during the experiments and the network usage required.

### **4.1 Protocols and Implementations**

Among protocol properties that have an effect on SPIT we look at how addressing is done as well as the synchronous nature of RTP. In terms of implementations we look at how voice mail, anonymity and long distance costs impact SPIT.

#### **4.1.1 Addressing**

As we noted in Section 2, SIP inherits its addressing from the e-mail system. SIP addresses comprise usernames at domains. The primary implication of this addressing in regards to SPIT is that techniques used by spammers to gather e-mail addresses can be used unmodified to also gather SIP addresses. SIP addresses can be extracted from web pages, mailing lists and newsgroups using the same crawlers already employed for e-mail address harvesting. Moreover brute force and dictionary attack techniques can be just as effective with SIP. We find from our experiments that guessing addresses is easier with SIP as the providers we studied issue sequential numeric aliases to user addresses. Thus, a SPITter who signs up and is issued an alias 555555@sip-r-us.com is certain that all six digit numbers below 555555 are assigned and therefore sending SPIT to those addresses is likely to reach users.

#### **4.1.2 Real Time Transmission**

A property of the Real Time Protocol which may have an impact on SPIT is its real time transmission. To send a thirty second message, a SPITter is required to transmit voice packets for thirty seconds and cannot simply package sound files and send to users. Although this could be used to deter SPIT, as it is SPITters can easily overcome this challenge by employing parallelism: sending

messages to multiple users simultaneously. We further explore the synchronous nature of RTP in the techniques we propose to deal with SPIT in Section 5.

#### **4.1.3 Voice Mail**

We find that two of the SIP providers in our study offer free voice mail service to their users. A third offers "paid for" voice mail. Voice mail has the effect of augmenting users' vulnerability to SPIT. With voice mail, even offline users can be reached by SPITters as messages are buffered at the voice mail.

In addition, our findings are that providers offering free voice mail forward these, in the form of sound files, to their users' e-mail accounts. This has the effect of exporting the SPIT problem to compound the already unsolved e-mail spam problem, providing a trusted relay (the provider's proxy) through which spammers can reach users. This can have a significant impact on the already overwhelmed e-mail system as voice files have significantly large sizes than text spam messages.

#### **4.1.4 Anonymity and Reach**

SIP offers similar anonymity facilities as those offered by e-mail. This obviates that VoIP's vulnerability to SPITters differs from that of the traditional circuit switched telephony. In the traditional telephony it is straightforward for law enforcement agencies to track down callers through their carriers. SPITters, however, can employ the same techniques as e-mail spammers such as using bot-nets as relays for their messages thus obfuscating their true locations. Bot-nets are assembled through, for example, use of worms that conquer vulnerable hosts globally.

In the U.S., spam on telephone is currently regulated by the Telephone Consumer Protection Act (TCPA) [11] which prohibits the use of automated devices for dialing unsolicited calls and through which the Federal Trade Commission (FTC) implements a Do Not Call Registry [12] making it illegal to call numbers in such registry. Because VoIP offers virtually free worldwide calling, it is nearly impossible to enforce such legislation as calls are just as likely to be originating from rogue distant locations as they are likely to be originating from the callee's neighbour.

Forging caller IDs is also effortless in VoIP since this is provided to the callee through the INVITE message assembled by the caller. Even if

proxies authenticate call initiations, SPITters can legitimately purchase telephone numbers in any local area such as that of the callee to gain their trust. As evidenced in the Associated Press article of [29] subscribers are known to trust caller IDs even though these can be forged. This is an area in which SPIT, scams and frauds come together. For example, it is noted in the article above that many credit card companies authenticate newly issued cards by caller ID. The article further reports on a fraud scheme in which fraudsters in possession of stolen credit cards spoof the caller ID of the credit card's owner to make money transfers using services such as Western Union. A phishing attack involving VoIP has been reported recently in [19] in which phishers lured users of a bank into calling a VoIP number and signing in with their account and PIN numbers in order to verify personal information.

Because of inexpensive worldwide calling VoIP subscribers should expect larger volumes of unsolicited calls. In effect, VoIP extends the reach of SPITters who not only have access to their local regions but much of the world. This imposes a challenge in enforcing any existing legislation.

## 4.2 Observed SPIT

From the SIP experiment which lasted for one and a half month only one call was received. The call was received on day 28 of the experiment. We were able to ascertain that this call was initiated by a human caller and not an automated dialer.

From this result we conclude that SPIT is not yet a problem in the SIP networks in study. This conclusion is reinforced by responses we received during our interviews with the SIP network administrators in which both report not having received complaints of SPIT activity in their networks.

From the Skype experiment, our experience differs considerably. Both user accounts we created received an unsolicited call within their first hour online. All calls received were initiated by human callers which indicates that autodialers are no yet in use. For the majority of the calls we are unable to determine their motivation. In Skype our accounts were also contacted by means of text. Some of these messages promoted online web sites.

Figure 2 shows the average number of calls our Skype user accounts received each day. The

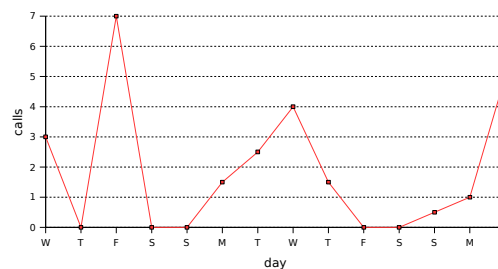


Figure 2. Average calls received on Skype

number of calls any one account received on a day varied between zero and nine. A weak pattern that can be seen in the figure is that the volume of calls received in weekends is generally low.

### 4.2.1 Network Usage

For the SIP call we received, we measured an incoming network usage of 21kbps. For Skype, the bandwidth usage of incoming packets was 51kbps. Other implementations would generate network traffic somewhere in between these reported.

At 21kbps, a 30 second SPIT message would require approximately 76KB. On average a 30 second message is expected to contain near 100 words [13], the equivalent of the average number of words per message we encountered by looking at near 100 spam e-mail messages.

To a SPITter this means that sending 100,000 voice messages a day, each having 30 seconds in length, requires 7.2GB of uplink network usage. We expect this to be a deterrent to home-grown SPITters, thus limiting the volumes of SPIT. We further discuss in Section 5 a technique that exploits the bottleneck of SPITters network uplink.

### 4.3 Preparation for SPIT

From the interviews with the SIP providers' administrative staff, we conclude that neither of the providers has in place mechanisms to deal with a possible surge of SPIT. However, administrators at both networks report that, although they have not encountered SPIT, the situation may change as VoIP gains popularity. We can sum up their opinion with the following quote from one of the administrator:

"I am not aware of anyone sending massive voice spam (like recorded advertisements). This is theoretically quite possible. We do not currently have any systems in place to prevent it."

These findings further reinforce our belief that SPIT can grow to become a problem on VoIP, unless mechanisms are in place to deal with it.

We thus conclude from these findings that VoIP users are vulnerable to SPIT just as e-mail users are. Although this is not yet a noticeable problem, we expect SPIT to grow as VoIP reaches the masses. At the moment little is being done in anticipation of a surge in SPIT, however, and we see this as the opportune moment to put measures in place in anticipation of this surge.

## 5 RECOMMENDATIONS

We detail two techniques to deal with SPIT. The first, we believe to be effective fighting automated dialers, whereas the second is a first step in dealing also with human callers.

### 5.1 Audio CAPTCHAs

Based on experiences collected from work on combating e-mail spam and based on our finding that VoIP offers a fertile space for SPIT to grow, we believe that the best way to deal with SPIT is by introducing a cost to SPIT. Techniques used thus far for e-mail spam such as client and proxy level filtering (including white and black lists) place the cost of dealing with spam on the receiver and the receiver's e-mail provider alone. Service providers must bear the cost of provisioning their servers to filter and handle additional mail loads caused by spam. Receivers must occasionally delete spam that gets through to their mail box and must periodically verify their spam folders to ensure no legitimate mail is lost. Meanwhile the only cost to spammers is that of network access, which is very low and fixed; i.e. the per-message cost of spam decreases with more messages, a clear incentive to send more messages. In increasing cost to SPITters, it is important to also ensure that legitimate callers are not significantly impacted by the measures, and that no unreasonable effort is required of callees and providers, as any of these would hamper the adoption of the technique.

We note that being a synchronous medium, telephony readily supports challenge-response authentication mechanisms. When receiving a call, the the user's device or proxy can request the caller to validate that he is human before allowing the call through to the callee. In this context, the caller could be challenged with a request to enter the letters and digits of a distorted audio recording. We propose that this solution be implemented at the proxy rather than the end user devices, as this set up allows for upgrades.

The generation of these recordings can take three modalities: the recordings may be automatically generated on-the-fly at the proxy, they may be randomly selected from a proxy-wide pool of pre-recorded tracks, or alternatively users may individually set their own recordings. The latter option is, however, not advised as it requires some user effort. Automatically generated recordings is a feasible approach as proxies can employ modified speech synthesizers which introduce noise and distortions in audio tracks. This technique, known in the text and graphics world as Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), has been shown in [38] to be effective with images that embed distorted text. Von Ahn et al show that CAPTCHAs are effective because they employ open AI problems such as recognition of distorted text and context from images. In our case we employ the same principles by exploiting the limitations of modern day speech recognition.

Audio CAPTCHAs could also be designed to consist of multiple recordings which can combine to form a context. For example playing multiple single sentence recordings such as "All vehicles must stop at crossings", "The steam engine fuelled the Industrial Revolution" and "Locomotion is a jazz standard from the 40s" should disperse the word "train" on a human caller. Determining context from speech is a harder AI problem than speech recognition alone, and we expect it will remain difficult for computers to solve for the next few years.

Audio CAPTCHAs can eliminate automated calls and we see it as discouraging for SPITters as it increases their costs of sending messages. They now ought to employ humans to decode the CAPTCHAs for each call, a relatively expensive undertaking which also limits the number of calls they can make. Thus the use of audio CAPTCHAs is effective to deal with automated voice calls, which are of most concern. Telemarketing calls are not addressed by the technique, however, and we discuss next a first step in that direction.

### 5.2 Proof of Commitment

Although we propose audio CAPTCHAs as the front line of attack against SPIT, we may employ in addition other techniques to reduce telemarketing calls. Proof of commitment is one

such technique which requires that the caller show commitment to the call before the call is allowed. An implementation of this technique could simply apply the rule "before I accept your call you must send me a 300KB header". More sophisticated proofs could be used, however this suffices for the purpose of our discussion. For the average caller making and receiving under 10 calls a day a 300KB proof of commitment per message would total a 5MB overhead a day with 6s delay per call on a 384Kbps link. For a SPITter, to make 100,000 SPIT calls of 30 second length each, would require a total of 35GB of upload bandwidth of which 28GB would be pure overhead from the proof of commitment. Because upstream bandwidth is generally more constrained than downstream this approach makes the spammer's bandwidth a bottleneck. For example, a typical Internet access plan offering 3Mbps downstream bandwidth is limited to 384Kbps upstream [32], and on such network nearly 9 days would be required to make 100,000 SPIT calls (even when employing parallelism).

This technique increases the cost of telemarketing calls, helps eliminating home grown SPITters and makes bots discoverable as drastic changes in daily bandwidth usage can be noticed by ISPs.

## 6 RELATED WORK

To the best of our knowledge, there has not been an attempt at understanding the emerging trends in SPIT. There are, however a number of alarming news articles warning of a grim future with SPIT [22, 7, 17, 9, 5, 8, 21]. Research in the area of defense against SPIT has initiated and we discuss the different approaches employed next.

Two research efforts most similar to ours deal with SPIT detection and are presented in [31] and [30]. Both works propose reputation based systems to address SPIT. The reputation of a caller is derived from past history with callee and inferred from trusted neighbours who may have had contact with the caller. However, reputation based techniques have been shown to be easily circumventable by colluding peers [25, 24]. SPITters can also game reputation systems by, for example, signing up for legitimate accounts at trusted providers, calling those accounts from rogue addresses in order to improve their reputation and then spam all users. Moreover,

SPITter accounts making use of bot nets will mostly have no history and therefore cannot be flagged as SPIT. Filtering all calls for which no reputation is built would block new users of VoIP from making calls whatsoever. Lack of built reputation gives no guarantees that the caller is a SPITter and only allows for suspicion. Another weakness of reputation systems is that malicious users can damage the reputation of a legitimate provider by signing up for accounts there and making spam calls. Lastly, reputation based techniques fail to provide a deterrent for SPITters. SPITters see no cost of making random calls.

A number of techniques have been applied in the combat against e-mail spam. Content based filtering allows providers or clients to flag spam based on its contents. This technique can only apply for voice calls when dealing with voice mail as no content is available until the call is accepted. Even so, it has been shown not to be effective at combating e-mail spam as the receivers bear all costs of dealing with spam and spammer has no deterrent. Whitelisting allows users to accept e-mails only from known parties, however this technique is rarely used because it prevents social networking. For example, this technique would not allow a researcher interested in another's work to contact him. Black listing is ineffective as SPITters with dynamic IPs or with access to bot-nets will always be able to spam users.

Qovia, a VoIP management software maker, has applied for a patent on a technique to broadcast VoIP calls, and claims it will use the patent to prevent SPITters from broadcasting calls [22]. The company fails to realize however that it will be impossible for them to enforce any such patent as SPIT could be sent from bots hiding the true identity of the SPITter, as well, they may just as easily be sent from foreign jurisdictions.

CAPTCHA has been proposed for use with text and images and have been effectively adopted by web sites in preventing bots from signing up for user accounts [26]. However, it is not applied against e-mail spam because e-mail is asynchronous. We make the observation that telephony is a synchronous medium which enables the integration of CAPTCHAS with little overhead for its users.

## 7 FUTURE WORK

In future, we propose to implement and evaluate the techniques we proposed here: audio CAPTCHAs and proof of commitment. A proper evaluation of these techniques will include their deployment in the real world to gain an understanding of how intrusive they can be to legitimate callers, what overhead audio CAPTCHAs impose on proxies and how well these techniques scale. To validate the effectiveness of the techniques in dealing with SPIT we intend on employing simulations, since SPIT is not yet common.

## 8 CONCLUSION

In conclusion, we have discussed the present state of spam on Internet telephony, we have looked at properties of the new medium that favour and those that challenge SPIT. We have made recommendations on techniques we judge effective in dealing with SPIT. Both our proposed techniques reduce SPIT at the source, by providing a deterrent to spam, which we believe to be the first steps in the right direction. Finally, we have given an overview of research directions being adopted in the combat against SPIT.

## References

- [1] AOL TotalTalk. <http://www.totaltalk.com/>, April 2006.
- [2] Associated Press. When a stranger calls, Caller ID may not be trustworthy. <http://www.startribune.com/484/story/278518.html>, March 2006.
- [3] S. A. Baset and H. Schulzrinne. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. *Columbia University Technical Report*, 04(39), Sept. 2004.
- [4] A. Baxter. Shtoom. <http://divmod.org/projects/shtoom>, April 2006.
- [5] A. Bhimani. Securing the commercial Internet. *Communications of the ACM*, 39(6), June 1996.
- [6] C. Bieber. Move over spam, make way for "spit". <http://www.newscientist.com/article.ns?id=dn6445>, September 2004.
- [7] P. Biondi and F. Desclaux. Silver needle in the skype. In *Black Hat Europe 2006*, Amsterdam, The Netherlands, Mar. 2006.
- [8] B. Charny. Net phone customers brace for 'VoIP spam'. <http://news.zdnet.com/2100-9584-22-5302988.html>, August 2004.
- [9] B. Charny. Alliance wants to beat spam to Net phones. <http://news.com.com/Alliance%20wants%20to%20beat%20spam%20to%20Net%20phones/2100-7352.3-5566267.html?part=rss&tag=5566267&subj=news.7352.5>, February 2005.
- [10] P. Cochrane. VoIP spam—it's coming. <http://news.zdnet.com/2100-1009.22-5359987.html>, September 2004.
- [11] Comcast Digital Voice. <http://www.comcast.com/benefits/voicebenefits.ashx>, April 2006.
- [12] A. Copestake. Augmented and alternative nlp techniques for augmentative and alternative communication. In *Workshop on Natural Language Processing for Communication Aids (ACL/EACL'97)*, Madrid, Spain, July 1997.
- [13] R. Dantu and P. Kolan. Detecting spam in voip networks. In *USENIX Steps for reducing Unwanted Traffic on the Internet Workshop (SRUTI '05)*, Cambridge, MA, July 2005.
- [14] EarthLink trueVoice. <http://www.earthlink.net/voice/truevoice/>, April 2006.
- [15] Ethereal Network Protocol Analyser. <http://www.ethereal.com/>, April 2006.
- [16] Federal Communications Commission. Unwanted Telephone Marketing Calls. <http://www.fcc.gov/cgb/consumerfacts/tcpa.html>, November 2005.
- [17] Federal Trade Commission. The National Do Not Call Registry. <https://www.donotcall.gov/>, April 2006.
- [18] C. Garretson. Qovia ready to take on VoIP spam. <http://www.networkworld.com/news/2004/071204qovia.html>, July 2004.
- [19] D. Geer. Will new standards help curb spam? *IEEE Computer Magazine*, 37(2), Feb. 2004.
- [20] A. Gonsalves. Phishers Snare Victims With VoIP . <http://www.techweb.com/wire/security/186701001>, April 2006.
- [21] S. Guha, N. Daswani, and R. Jain. An experimental study of the skype peer-to-peer voip system. In *International Workshop on Peer-to-Peer Systems*, Santa Barbara, CA, USA, Feb. 2006.
- [22] P. Korzeniowski. VoIP Emerging as Next Spam Entryway. <http://www.technewsworld.com/story/45518.html>, August 2005.
- [23] S. Kuchinkas. Spam, DoS Headed VoIP's Way. <http://www.internetnews.com/security/article.php/3398331>, August 2004.
- [24] Q. Lian, Y. Peng, M. Yang, Z. Zhang, Y. Dai, , and X. Li. Robust incentives via multi-level tit-for-tat. In *International Workshop on Peer-to-Peer Systems*, Santa Barbara, CA, USA, Feb. 2006.
- [25] Q. Lian, Z. Zhang, M. Yang, B. Y. Zhao, Y. Dai, , and X. Li. An Empirical Study of Collusion Behavior in the Maze P2P File-Sharing System . Microsoft Research Technical Report: MSR-TR-2006-14, February 2006.
- [26] C. E. Perkins. IP Mobility Support. <http://www.ietf.org/rfc/rfc2002.txt>, October 1996.

- [27] M. K. Powel. Remarks of michael k. powell chairman federal communications commission at the national association of regulatory commissioners. [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-244737A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-244737A1.pdf), March 2004.
- [28] Y. Rebahi and D. Sisalem. Sip service providers and the spam problem. In *2nd Workshop on Securing Voice over IP*, Washington DC, USA, June 2005.
- [29] Rogers Cable. <http://www.rogers.com/>, April 2006.
- [30] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. <http://www.ietf.org/rfc/rfc3261.txt>, June 2002.
- [31] S. Savage, N. Cardwell, D. Wetheral, and T. Anderson. TCP congestion control with a misbehaving receiver. *ACM SIGCOMM Computer Communication Review*, 29(5), Oct. 1999.
- [32] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. <http://www.ietf.org/rfc/rfc3550.txt>, July 2003.
- [33] Skype. <http://www.skype.com/>, April 2006.
- [34] A. C. Snoeren and H. Balakrishnan. An end-to-end approach to host mobility. In *ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 00)*, Boston, MA, Aug. 2000.
- [35] Twisted Matrix Laboratoris. Twisted Matrix. <http://twistedmatrix.com/trac/>, April 2006.
- [36] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford. Captcha: Using hard ai problems for security. In *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2003)*, Warsaw, Poland, May 2003.
- [37] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford. The Captcha Project. <http://www.captcha.net/>, April 2006.
- [38] Vonage Fast Facts. <http://www.vonage.com/corporate/aboutus.fastfacts.php>, April 2006.
- [39] Zope Corporation. Zope. <http://www.zope.org/>, April 2006.