# Prevention of Unsolicited Voice Calls in the IP Multimedia Subsystem

David Waiting and Neco Ventura
{david, neco}@crg.ee.uct.ac.za
University of Cape Town, Rondebosch, South Africa

***Abstract*— The IP Multimedia Subsystem is an overlay architecture for all-IP based core networks. With the introduction of this packet-based telecommunication implemented on top of various network technologies, we see an increase in connectivity and network efficiency, and a decrease in costs.**

**In the past users have become accustomed to paying for voice calls but recently we have seen the increasing popularity of free Internet-based voice calls. It is envisaged that IMS will further decrease the barriers to ubiquitous cheap voice communication. What has since emerged is a problem that has received little attention in previous research: unsolicited voice calls, otherwise known as spam over Internet telephony. In this paper we demonstrate the power and flexibility of the IP Multimedia Subsystem and show that with the correct service provisioning we can solve the problem of unsolicited voice calls before it escalates to the same levels of email spam.**

## I. Introduction

There is an increasing trend to move towards all-IP based network architectures. All-IP networks allow for greater flexibility, lower costs, and a simpler road-map towards the eventual goal of fixed-mobile convergence. In order to smooth the transition between traditional circuit switched networks to the packet switched domain the 3GPP has standardised the IP Multimedia Subsystem (IMS) [2]. The IMS provides a single service delivery platform that facilitates seamless service delivery across many different access technologies, including UMTS, WLAN, GSM and ADSL, while still fully supporting legacy PSTN networks.

It has already been shown that providers such as Skype have captured a large market of Internet telephony users, and as such are slowly eroding the divide between voice and data communication. Whereas previously we would employ a telephone to make voice calls and a PC to send emails and browse the Internet, we now see users making calls from their PCs, and sending emails from their telephones. Not only are these new technologies making communication more accessible but also significantly cheaper. An unfortunate result is that with very cheap (or in some cases free) telephony there is ample opportunity for misuse.

Every year the world sees an increase in the number of spam email and instant messages sent, and this can only indicate that sending spam is financially profitable [10]. When the costs of packet-based telephony decrease to a certain threshold then SPIT (Spam over Internet Telephony) will become a reality [8]. Moreover, while deleting a few unwanted emails every day does not take a significant amount of time, answering just a few unsolicited calls each day could consume huge amounts of time and be the source of a great deal of frustration. Already users of Skype have complained that they are receiving unsolicited calls, mostly from other users looking for companionship. Even with a fairly modest PC a spammer could initiate thousands of unsolicited calls in a day [4].

Due to the fact that the IMS is a relatively new technology, we begin this paper by presenting an overview of the key components of the IMS architecture, and show the basic call setup procedure. We then go on to show why we believe that SPIT will become such a large problem by highlighting the prevalence of email spam, and show some of the mechanisms deployed thus far to try and reduce spam. Following that, we present a proposal for detecting SPIT, and show how it integrates into the IMS architecture.

## II. Session Setup in the IMS

The IMS offers an architecture that allows for multimedia service provisioning across several different access technologies - both wired and wireless. It was originally defined in Release 5 of UMTS, and was extended in Release 6 for ease of implementation (including the provision for using IPv4). Moreover, the 3GPP2 has also adopted the architecture for use on top of their Multimedia Domain (MMD) [2].

An IMS user is contactable by their Uniform Resource Identifiers (URI) that utilises a similar convention to email address, e.g. sip:foo@bar.com. Users need only have one URI to be accessible from many locations and the URI may refer to user's land-line, cellular telephone, or softphone, depending on their presence status. It is possible for a call addressed to a single URI to make all three devices ring simultaneously. Usually a user would register their current location with a registrar, and thus be accessible regardless of the terminal they are using. This notion of a universal address makes it all the more valuable to spammers.

### A. IMS Overview

The IMS utilises several existing protocols including the Session Initiation Protocol (SIP), Diameter, Session Description Protocol (SDP), the Real-time Protocol (RTP), and many others. While the IMS does provide support for traditional circuit switched networks via gateways, the aim is to move all signalling and media transport to the packet switched domain. This will facilitate convergence as well as reduce both operating and capital expenditure for service providers,

due to cheaper infrastructure and reduced complexity. Services such as VoIP, multimedia conferencing, and push-to-talk are provisioned using an all-IP delivery environment.

The IMS architecture dictates that signalling information and media data do not necessarily follow the same path through the IP network. In most cases once a call has been setup the actual media will follow an optimised path between caller and callee, and be transported using a suitable protocol such as the RTP. In addition to this, once an initial invite request has been received by a callee, additional signalling does not necessarily need to follow the same path through the various SIP proxies. Unless a SIP proxy specifically requests that it be part of the signalling path, by setting a record-route header in the SIP message, it may be missed by future messages.

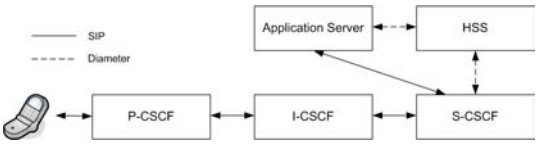


Fig. 1. IMS core components.

In Fig. 1 the key components for an IMS call setup are shown. The proxy call session control function (P-CSCF) is the entry point into the IMS and can either be on the user's home network or may be located on a visited network. The P-CSCF forwards requests, maintains security associations with the UE, and enforces local policies. Typically the P-CSCF can be discovered through either DHCP, or in the case of mobile terminals, during the GPRS PDP establishment. The primary function of the interrogating CSCF (I-CSCF) is to assign a serving CSCF (S-CSCF) to a user, but may also act as a topology hiding inter-network gateway. The S-CSCF acts as a registrar and a SIP proxy. Since the S-CSCF also collects session information about billing it remains on the signalling path.

The home subscriber server (HSS) contains all user information including the user's public and private identities. It also maintains authentication information and can assist the I-CSCF to select an appropriate S-CSCF. Application servers facilitate service provisioning by either acting as a UA, redirect server, or a SIP proxy. Network providers have the choice to implement services using CAMEL, SIP, or OSA/Parlay application servers.

### *B. Call Setup Procedure*

To initiate an IMS call the caller's UA sends a SIP Invite to the P-CSCF that is then routed through the IMS core to the callee's UA. The destination UA would typically respond with a ringing response until the call is answered after which the UA would send a 200 OK response indicating that the call has been answered.

Figure 2 shows a typical call setup procedure. For simplicity neither the CSCFs nor any QoS signalling is shown.

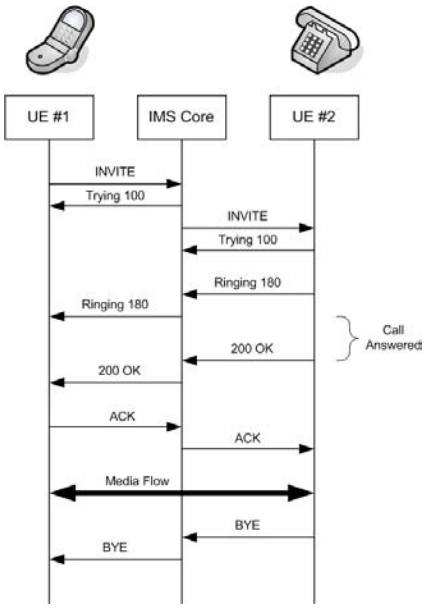


Fig. 2. Basic call setup.

## III. SPAM

In order to visualise the potential problems that SPIT will cause we need to evaluate the problem of email spam. Most spam messages contain harmless commercial advertising although some, more dangerous, spam attempts to defraud users using scams and phishing attacks [5]. Spammers identify their targets by scanning Usenet postings, stealing Internet mailing lists or simply searching the web for addresses. Spam costs very little to send since most costs are carried by the recipients and the carriers, and the marginal costs of sending millions of spam messages are almost zero.

In March 2006 Integrated Message Management company Postini processed over 23-billion email messages, of which it was found that 19.6-billion were spam - thus a total of 84% of all email was unwanted [10]. In the last 6 months Postini has processed 131,5 terabytes of spam. These statistics indicate the huge problem that spam has become worldwide. While spam is an annoyance for those that receive it, spam also causes unexpected overloads in network bandwidth, storage capacity and reduces end-user productivity.

Many solutions have been proposed to combat the rising prevalence of spam. These can be summarised in the following categories:

### *A. Legislation*

The European Union, the USA and South Africa have all passed laws dealing with unsolicited email. The well-known CAN-SPAM act of 2003 established national standards in the USA for sending commercial email. The act requires senders of commercial marketing to clearly provide opt-out mechanisms, valid subject-line and routing information, and a legitimate physical address of the mailer. Critics of the act

suggested at the time that legislation actually encouraged spam because every company was legally entitled to at least one shot at every email address.

South Africa's own Electronic Communications and Transactions Act of 2002 permits marketers to send unsolicited email as long as the consumer is given the option to cancel his or her subscription.

Current legislation states that sending spam is legal, and does little to prevent against fraud. Moreover, enforcing such legislation is very difficult due to anonymity of the Internet. Since the adoption of the CAN-SPAM act the amount of spam in the Internet has in fact increased [15], demonstrating that legislation does little to curb this problem.

### B. Sender-based Filtering

Many ISPs have adopted the technique of filtering out potential spam messages based on the origin of the email. This entails storing large databases of known spammer domain names and discarding their messages. However, not only do these lists require constant updates but it is possible to conceal the true origin of email through the technique of spoofing. Therefore the origin of email must be authenticated for these techniques to work effectively. Unfortunately the mere fact that the source of the email has been authenticated does not necessarily indicate that the message is not spam [3]. Spammers acquire throwaway domains, referring to the practise of using authenticated email accounts to send spam and then moving to a new domain when the previous one is blacklisted.

### C. Statistical Filtering

Bayesian email filters have been implemented in software such as Mozilla Thunderbird and SpamAssasin. Bayesian spam filters examine the contents of email messages and determine the probability that a particular message is spam by examining a large corpus of previous emails that are known to be either spam or non-spam. Certain words have a higher probability of occurring in spam-email than in non-spam email. If an email contains a large percentage of 'spam words' then it is marked as spam and possibly deleted.

Bayesian filters have been shown to catch up to 99% of spam messages [6], however, these filters are susceptible to false positives. Most users would prefer to receive 100 spam messages than to lose a single legitimate message.

### D. Payment

Most spam is sent because it is financially profitable to do so. Studies have shown that a response rate as low as 1 in 100,000 allows spammers to recover their costs [11]. Various individuals have suggested that in order to eliminate spam the sending of email should incur some kind of cost. Obviously this is a very contentious issue as some people would prefer to live with spam than to have to pay to send email.

Companies such as Goodmail Systems offer a service that allows email senders the option of bypassing spam-blocking software on well-known email servers (such as AOL) for a certain fee. Only accredited companies would be allowed to use the system, and as such the emails are guaranteed to have neither spam nor phishing content. Critics of the technology call it paid-for spam.

## IV. Detecting Spit

We have identified various methods in which voice spam can be detected and these are summarised below.

### A. Blacklists

The SMTP protocol used for sending email messages is inherently insecure. The headers of the email message can carry false information, otherwise known as spoofed addresses [7]. In the IMS a user cannot spoof addresses because of the security mechanisms that the IMS employs, and because a UA needs a valid IP address for any media to flow between the communicating parties. Therefore blacklists of known spammers can be stored on the HSS, and S-CSCF servers can easily terminate these calls before they reach an end user. Unfortunately, as has been shown with our experiences of email, blacklists can never be kept up to date, and spammers will change their URIs and IP addresses as often as necessary to avoid being blocked. Therefore, while this server-side service will offer some protection, it is not adequate solution on its own. A blacklist implemented on the individual's UE is useful to block certain unwanted callers according to the user's preferences.

### B. Whitelists

It is possible to configure end-users UA software to accept calls only from known SIP URIs or trusted IP addresses. This would ensure that users would never receive unsolicited calls. However, most people want to accept calls from just about anyone - provided these calls are legitimate. It is clear that a whitelist approach limits the functionality of IP telephony too much for most users.

### C. Statistical Filtering

It is possible to adopt a similar approach to the Bayesian filtering of email for SIP messages. A UA can examine the SIP signalling messages received from a caller trying to establish a session and perform statistical filtering in order to determine whether the incoming session has the characteristics of a spam session. For example the return routes listed in spam SIP headers from foreign countries might look quite different from calls that a user usually receives from local friends and family. In a similar fashion to modern email clients, a user would have the option to flag a call as SPIT, and train the filter to better identify SPIT at a later stage.

While it would be very difficult to identify SPIT from the actual contents of the media stream in real-time, it is possible to perform statistical filtering on messages stored in a user's voice mailbox. Filters could be trained to identify keywords via voice recognition software, and either delete the messages or mark them as low-priority.

### D. Turing Tests

The detection of voice spam can be harder than the detection of email spam because IP telephony is a real-time application. There is less time in which to process the data and the contents of the media stream is not known *a priori*. However we can use the fact that voice is a real-time application to identify unsolicited calls.

Email challenge-response systems issue a challenge to a user wishing to send a message. The challenge will usually be quite simple, but ensures that the person initiating the message, has a valid email address, is an actual person, and is concerned enough about the message to warrant spending a little time to ensure that it is delivered. Challenge-response systems have been proposed to counteract email spam, but the system is cumbersome in a non-realtime environment, and slows message delivery considerably [14].

In order for SPIT to be profitable, spammers would need to initiate thousands of voice calls a day to market their products. This could only be done with the aid of computer-generated calls, most likely with some pre-recorded message. We propose that a challenge-response system for IP telephony would reduce the quantity of SPIT because only human users would be able to place calls.

## V. Challenge-Response Mechanism

The challenge-response mechanism that we propose requires no changes to existing UE, and only requires network operators to install a single application server capable of handling many requests simultaneously.

### A. Spittoon

In our system, called *Spittoon*[1], the user's home network maintains a whitelist on the HSS of their trusted correspondents. During call-setup the S-CSCF checks a user's whitelist, and if the call is initiated from a location that does not appear on the whitelist then it is forwarded to an application server acting in UA mode. The application server issues an automated Turing test challenge to the caller. The Turing test software generates tests that it itself could not pass. This concept has been often been applied to well-known email services such as Yahoo and Hotmail, which require users to pass a visual Turing test before registering on their sites, blocking bots from signing up hundreds of email accounts.


Fig. 3. A visual Turing test.

Figure 3 shows a typical visual Turing test. It is based on human's ability to read distorted and overlapping text, while computers cannot. Audio Turing tests work in a similar way. A word or sequence of numbers is chosen at random, which is then rendered to form a sound clip. The sound clip is then distorted and possibly overlaid with other background noise. In our system a random 5-digit number is used. Once the clip has been played the user is then required to key in the number using the phone-keypad, which is transmitted to the application server via either SIP INFO messages or RFC2833 DTMF signals.

[1]Def: spittoon - *noun.* A receptacle for spit.

### B. Call Setup

If the user enters the correct sequence of numbers the caller is added to a user's whitelist and the call is transferred to the intended original destination. Entries in the whitelist never expire and must be specifically removed by users if they are no longer wanted. Call transfer in SIP sessions is implemented in a decentralised manner. Thus, the application server requests that the caller initiate the new connection and the original call is ended separately [12].

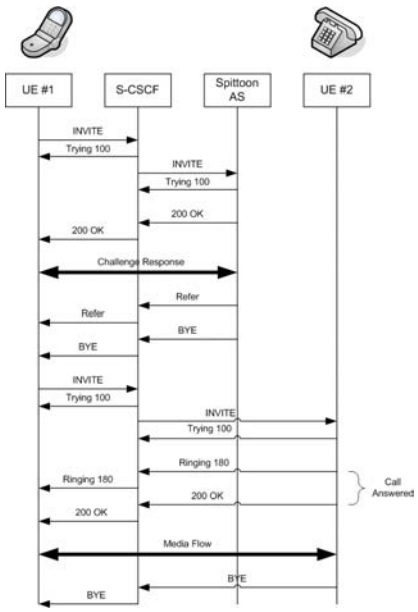


Fig. 4. Successful call setup using spittoon.

Figure 4 shows the signalling that takes place when using Spittoon. Only the UAs, S-CSCF and application server are shown. QoS signalling and ACKs are omitted from the figure. After the Transfer method is sent to the caller the application server terminates the challenge-response session using a blind transfer. The blind transfer differs from an assured transfer in which a new session is initiated before the previous one is ended [2].

If the challenge-response test is failed then the caller is not added to the callee whitelist and no call can be placed. The caller does have the option to retry the test a number of times before the caller's identity is blacklisted permanently.

This technology can just as easily be extended to video conferencing and push-to-talk sessions, although we do not consider these services in this paper.

### C. System Overheads

The Spittoon system does add additional overheads to the core network since all unauthenticated callers must first be routed to the Spittoon server. However, the additional one-time overheads of the Spittoon service are justified due to the overall reduced network load due to a fewer number of unsolicited calls being routed to end users.

The worst overhead is the waste of time for legitimate callers. As such the system the system will be incorporated with an algorithm to identify high-risk callers and only expose them to the challenge-response test. This algorithm is left for future work.

### D. Challenges

While the proposed system does eliminate the calls originating from automated systems, it still does not eliminate all unsolicited calls. There will still be marketers that choose to place calls using humans, or simply get humans to solve hundreds of challenge-response tests every day, and in the process get added to user's whitelists. However, the opportunity exists in current PSTN systems for this type of marketing, and as yet it has not proved to be a significant problem in most countries. Another problem is that the system does not prevent strangers seeking companionship from placing calls as they please. Unfortunately the nature of voice communication is that no-one really knows if they want to receive a call until they have already received it.

## VI. Related Work

While research into SPIT is still in its infancy there are various related works worth highlighting.

### A. Turing Tests

Researchers at the Carnegie Mellon School of Computer Science are involved in the CAPTCHA project, which stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart [13]. A CAPTCHA is a test that is generated by a computer that it itself cannot pass, similar to the one shown in Fig. 3. As mentioned previously, their work is mostly used by free email services such as Yahoo to stop bots from registering thousands of accounts. However, they identify alternate uses for their technology for online polls, thwarting search engine bots, reducing spam, and preventing dictionary attacks on password encrypted systems.

Part of their research includes trying to solve these CAPTCHAs using AI technology. Other researchers have shown that computers have been able to solve CAPTCHAs with reasonable accuracy with modern shape context matching technology [9]. It is a constantly evolving field of research, with harder tests being generated and smarter algorithms being designed to solve them.

### B. SPIT

The FOKUS group performs a great deal of research into IMS related issues [1]. Their IMS playground is a valuable tool for industry and academics to test the latest IMS technologies in a practical environment. In their March 2006 newsletter they discuss current research into IMS security measures and describe their intentions to create a SPIT prevention mechanism using Bayesian filtering and reputation management, however, specifics of the project are not yet available.

Qovia of Maryland USA have filed two patent applications for technology to thwart SPIT [4]. Their technology identifies potential SPIT by the frequency and duration of calls.

## VII. Conclusions and Future Work

In recent years email users have found their mailboxes cluttered with unwanted spam. With the introduction of very inexpensive voice calls it is likely that the same problems will be experienced with VoIP. To prevent spammers from generating large quantities of unwanted calls a challenge-response mechanism must be implemented, such as the Spittoon server proposed in this paper.

We are currently implementing our server on a practical testbed for proof-of-concept trials. Future work includes extending this work to incorporate spam detection in video, push-to-talk, and instant message sessions.


## Acknowledgement

The authors would like to thank Telkom, Siemens, the National Research Foundation (NRF) and the Department of Trade and Industry (DTI) for supporting this research project.


## References


[1] Fraunhofer FOKUS - Institute for Open Communications Systems. http://www.fokus.gmd.de/.

[2] 3rd Generation Partnership Project (3GPP). IP Multimedia Subsystem (IMS). *TS 23.228*.

[3] Steven M Bellovin. Spamming, Phishing, Authentication, and Privacy. *Communications of the ACM*, 47(12):144, December 2004.

[4] Celeste Biever. Move over spam, make way for "spit". *NewScientist.com News Service*, September 2004.

[5] Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz. Anatomy of a Phishing Email. *Conference on Email and Anti Spam (CEAS)*, July 2004.

[6] Paul Graham. *Hackers and Painters*. O'Reilly, 2004.

[7] N.E. Hastings and P.A. McLean. TCP/IP spoofing fundamentals. *IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications*, pages 218–224, March 1996.

[8] Paul V. Mockapetris. Telephony's Next Act. *IEEE Spectrum Magazine*, April 2006.

[9] G. Mori and J. Malik. Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 1, June 2003.

[10] Postini. Postini Reports Increase in Unwanted Email and Instant Messaging Attacks During the Month of March. *http://www.postini.com*, April 2006.

[11] Claudia Sarrocco. Spam in the Information Society: Buidling Frameworks for International Cooperation. *World Summit on the Information Society (WSIS)*, 2005.

[12] Henning Schulzrinne and Jonathan Rosenberg. The Session Initiation Protocol: Internet-Centric Signaling. *IEEE Communications Magazine*, October 2000.

[13] Luis von Ahn, Manuel Blum, and John Langford. Telling Humans and Computers Apart Automatically. *Communications of the ACM*, 47(2):57–60, February 2004.

[14] Lauren Weinstein. Spam Wars. *Communications of the ACM*, 46(8):136, August 2003.

[15] Tom Zeller. Law Barring Junk E-Mail Allows a Flood Instead. *The New York Times*, February 2005.