SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam

Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn
Arizona State University
{tu, doupe, zzhao30, gahn}@asu.edu

***Abstract*—Telephone spam costs United States consumers $8.6 billion annually. In 2014, the Federal Trade Commission has received over 22 million complaints of illegal and wanted calls. Telephone spammers today are leveraging recent technical advances in the telephony ecosystem to distribute massive automated spam calls known as robocalls. Given that anti-spam techniques and approaches are effective in the email domain, the question we address is: what are the effective defenses against spam calls?**

In this paper, we first describe the telephone spam ecosystem, specifically focusing on the differences between email and telephone spam. Then, we survey the existing telephone spam solutions and, by analyzing the failings of the current techniques, derive evaluation criteria that are critical to an acceptable solution. We believe that this work will help guide the development of effective telephone spam defenses, as well as provide a framework to evaluate future defenses.

I. Introduction

The national and global telephony system is a critical component of our modern infrastructure and economy. In the United States (US), the mobile telephone subscribership penetration rate has already surpassed 100% [1]. According to the U.S. Bureau of Labor Statistics, each day more than 240 million hours are spent on telephone calls in the United States, equating to more than 88 trillion hours each year [2].

However, with the pervasiveness of telephone service subscribership, telephone spam has also become an increasingly prevalent issue in the US. Recent technical advances in the telephony ecosystem are leveraged by spammers to distribute massive automated spam calls, known as *robocalls*. The Federal Trade Commission's (FTC) National Do Not Call Registry's cumulative number of complaints of illegal calls in the US totaled more than 22 million in 2014 [3], with about 200,000 complaints each month about robocalls alone [4]. Despite US laws prohibiting robocalling and telephone spamming (with some exceptions), complaints on illegal calls have reached record numbers year after year, which indicates that the laws have not deterred the spammers.

Spam calls are significant annoyances for telephone users. Unlike email spam, which can be ignored, spam calls demand immediate attention. When a phone rings, a call recipient generally must decide whether to accept the call and listen to the call. After realizing that the call contains unwanted information and disconnects from the call, the recipient has already lost time, money (phone bill), and productivity. A study in 2014 by Kimball et al. [5] found that 75% of people listened to over 19 seconds of a robocall message and the vast majority of people, 97%, listen to at least 6 seconds. Even when the recipient ignores or declines the call, today spammers can send a prerecorded audio message directly into the recipient's voicemail inbox. Deleting a junk voicemail wastes even more time, taking at least 6 steps to complete in a typical voicemail system.

Telephone spam are not only significant annoyances, they also result in significant financial loss in the economy, mostly due to scams and identity theft. According to complaint data collected by the FTC, Americans lose more than $8.6 billion due to fraud annually, and the vast majority of them (and still increasing) are due to phone communication [4]. This situation is surprising, given the significant gains made in reducing the amount of email spam. This raises the question: *are there any simple and effective solutions that could stop telephone spam?* The unfortunate answer is no. We found that this issue is not easily solved, and, in fact, the simple and effective techniques against email spam cannot be applied to telephone systems. There are significant differences and unique challenges in the telephone ecosystem that require novel approaches. Many existing solutions have failed to overcome these challenges and, as a result, have yet to be widely implemented.

The objective of this paper is to survey the existing solutions in combating telephone spam and, by analyzing the failings of the current techniques, derive the requirements that are critical to an acceptable solution. This work will help guide the development of effective telephone spam defenses, as well as provide a framework to help evaluate the techniques against telephone spam.

The main contributions of this paper are the following:

- We describe the telephone spam ecosystem, focusing on the players involved and the technical challenges that make telephone spam distinct from email spam.
- We develop a taxonomy that classifies the existing anti-spam techniques into three categories, providing a high-level view of the benefits and drawbacks of each type of technique.
- We provide a systematization of assessment criteria for evaluating telephone spam countermeasures, and we evaluate existing techniques using these assessment criteria.

- We provide a discussion on what we believe to be the future direction of solving the telephone spam problem.

II. Background

While email spam is arguably the most well-known form of spam, telephone spam is now more popular than ever. The Public Switched Telephone Network (PSTN) is an aggregate of various interconnected telephone networks that adheres to the core standards created by the International Telecommunication Union, allowing most telephones to intercommunicate. We define *telephone spam* as the mass distribution of unwanted content to modern telephones in the PSTN, which includes *voice spam* that distributes unwanted voice content to answered phones, and *voicemail spam* that distributes unwanted voice content into the recipient's voicemail inbox.

Due to the much greater capacity of IP infrastructure and the wide availability of IP-based equipment, telephony service providers have shifted their network infrastructure to IP-based solutions, and the operation cost of the telephone network has dramatically decreased. While the core PSTN infrastructure has evolved to be almost entirely IP-based, the core signaling protocols have not changed. The entire ecosystem still relies on the three-decade-old Signaling System No. 7 (SS7) [6] suite of protocols, allowing any phone to reach any other phone through a worldwide interconnection of switching centers.

A very common way of disseminating telephone spam is *robocalling*, which uses an autodialer that automatically dials and delivers a prerecorded message to a list of phone numbers. An *autodialer* is a generic term for any computer program or device that can automatically initiate calls to telephone recipients. Today, an autodialer is usually a computer program with Voice over Internet Protocol (VoIP) connectivity to a high volume VoIP-to-PSTN carrier, that may include features such as voicemail and SMS delivery, customizable caller ID, Call Progress Analysis, scheduled broadcast, text-to-speech, Interactive Voice Response, etc.

The high reachability of telephone numbers has led to telephony being an attractive spam distribution channel. Almost every adult in the US can be reached with a telephone number, and the vast majority of telephone numbers are mobile telephone subscribers. Although VoIP usage has been growing rapidly, we found that it is more of an add-on protocol (instead of a wholesale replacement) of existing mobile wireless and landline services. Using 2013 statistics, there are about 335 million mobile telephone subscribers [1], 136 million fixed-telephone subscribers [7], and 34 million VoIP subscribers [8] in the US (population 318 million).

We believe the improved cost efficiency of telephone spamming, advancement of spam distribution technology, and high reachability of telephone numbers contributed to the recent surge in telephone spam. Furthermore, we believe that telephone spam has the potential to be more persuasive than email spam, particularly when spammers use techniques such as caller ID spoofing.

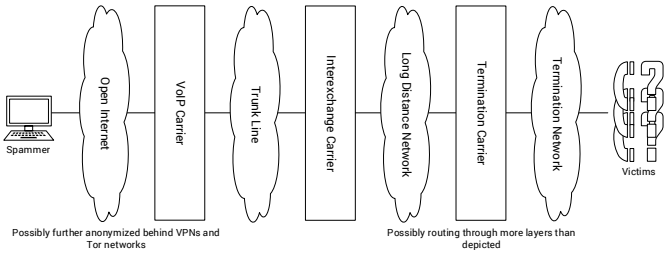

Figure 1: Routing of a spam call.

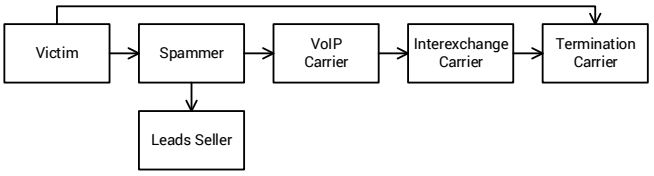

Figure 2: The flow of money in the telephone spam ecosystem.

A. Key Players of Telephone Spam

To understand the telephone spam ecosystem, we will first identify and explain the roles of all players who take part in the routing of a telephone spam. Figure 1 show a graphical depiction of the routing process: The spammer connects through the Internet to an *Internet Telephony Service Provider*, then the call is routed through an *Interexchange Carrier*, before finally being accepted by the *Termination Carrier*, who then routes the call to the victim.

Another way to understand the ecosystem is to show how money flows through the system, which we display in Figure 2: the money flows from the victim to the spammer, and the spammer uses this money to obtain leads (new phone numbers to spam) and to pay for the spam calls, the *Internet Telephony Service Provider* receives the money from the spammer and pays the *Interexchange Carrier*, who then pays the *Termination Carrier*. Next we examine each of these roles in turn.

Spammer is the agent that carries out the spamming operation. The spammer could be part of an organization, or an independent contractor that offers spamming-as-a-service. The goal of the spammer is usually to extract money from victims through sales and scams, or to launch a campaign of harassment. For cost efficiency, spam calls are typically initiated using an autodialer connected to an *Internet Telephony Service Provider* to reach the PSTN victims. Currently, spamming to VoIP victims are not as common, mainly due to the limited pool of potential victims, and some VoIP users, such as Skype, may not be reachable most of the time. We will describe the spammer's operation in more detail in Section II-B.

Internet Telephony Service Provider (ITSP), also known as a VoIP carrier, is a type of termination carrier that offers telecommunications service over the TCP/IP network, i.e. the Internet. The ITSP typically offers high volume calling at a lower cost compared to traditional carriers, and generates revenue based on the minutes of calls hosted. Whenever the spammer makes an outbound call to a PSTN number, the ITSP will convert the signaling protocol from VoIP to SS7, and route the converted signal through an interexchange carrier.

Interexchange Carrier (IXC), also known as a long distance carrier, is a cross-regional carrier that carries call traffic between telephone exchanges over long distances. The IXC charges its subscribers (mainly termination carrier such as the ITSPs and local mobile/landline carriers) for handling long distance phone calls and compensates the next-hop carrier (such as the recipient's termination carrier) for access. Unlike the peering model between Internet service providers [9], the IXC negotiates access rates with other carriers, known as intercarrier compensation. In the US, intercarrier compensation [10] is a complex system in which the rates vary according to traffic origination, location, carrier, and traffic type, and the rates are governed by federal and state regulators. In general, when two carriers are directly connected, the originating carrier compensates the next-hop carrier for routing the call in the next-hop carrier's network.

Termination Carrier, also known as local exchange carrier, is a carrier that provides call routing services within a local network that terminates at its end users. The termination carrier may be operating a landline, mobile, or IP-based telephone network. Most consumers and businesses rely on termination carriers for their telecommunications services. The termination carrier typically bills the IXC for the amount of incoming traffic, known as the access charge. In the US and some other countries, the recipient subscriber may also be partially billed for incoming calls.

B. Spammer Operation

Spamming (regardless of the medium) requires three basic elements: a recipient list, content, and a mass distribution channel. In addition, a more sophisticated spammer may employ circumvention measures to defeat spam countermeasures, and to avoid being stopped by law enforcement agencies.

1) Gathering Numbers: Spamming first requires a list of potential victims to contact, and in the case of telephone spam: a list of phone numbers. While there are many ways a spammer could gather phone numbers, the simplest method is to purchase the numbers from a leads seller. We did a simple Google search (keyword "leads for sale") and found hundreds of websites that offers access to millions of curated phone numbers for less than $100. There are also other ways to harvest phone numbers, such as crawling the web, collecting form submissions, downloading leak databases, covertly gathering through smartphone apps, or simply generating the numbers based on phone numbering plans. However, we do not know for sure the most popular means of obtaining a list of phone numbers for spamming, due to the lack of existing studies. Once the spammer gathers a list of phone numbers, the spammer can load it in an autodialer for mass distribution of the content.

2) Voice Spam Content: The content of telephone spam is typically a prerecorded audio stream made by either recording human voice or by using a text-to-speech synthesizer program. Telephone spam can also deliver interactive voice content, with the use of an Interactive Voice Response (IVR) system. When the recipient answers a call from an autodialer with interactive content, the recipient can interact with the system through voice and keypad inputs, and an automated voice message is played back based on the interaction.

There are a wide variety of spam types, such as telemarketing, impersonation scam, debt collection, political campaigns, one-ring scam, and so on. In order to provide insight into the telephone spam content, we collected 100 audio samples from various publicly available sources where audio recordings of voice or voicemail spam are uploaded. We perform this analysis to gain a general understanding of voice and voicemail spam, and we emphasize that, due to the biased method of data collection, these results do not constitute measurements that reflect trends on the whole of voice and voicemail spam. However, these results provide needed background and insight into the actual voice and voicemail spam. We will describe the following prevalent types of spam: credit card verification scam, fake tax agent scam, and political robocalls.

In the *credit card verification scam* samples, the called recipients are informed that their credit card account was deactivated, and they are asked to enter their credit card and social security number over the phone to verify their identity and get the account reactivated. While we only were able to listen to the audio of the call, based on comments from some of the uploaders, the scammers would spoof the caller ID to make it look as if the call originated from the credit card issuer. All of these scam calls used an Interactive Voice Response system to interact with the recipients and collect their credit card information. We found that the audio from the scammer's IVR system came from either a synthesized voice or *audio duplicated from the IVR system of the real credit card issuer*. From what we observed, the use of caller ID spoofing and sound duplicated from the real credit card issuer's IVR system made it almost indistinguishable from a real credit card verification call.

In the *fake tax agent scam* samples, the recipient receives a call from the scammer identifying himself as a tax agent of the Internal Revenue Service (IRS) and provides a fake badge number. The scammer proceeds to tell the recipient that he or she owes a specific amount of money to the

IRS. Often, the scammers demand immediate payment and threaten jail, deportation, or loss of driver's license if the victim does not pay. Based on the comments from the uploaders, the scammers would spoof their caller ID to make it look as if the call originated from a government agency by showing an area code from 202 (Washington, DC). These scammers seem to target immigrants [11]. We found that the majority used a live person to interact with the victim, and the rest used a prerecorded synthesized voice without an IVR system. One thing we noted was that all of the live person scammers had a South Asian accent, and in our opinion, the accent had made the call sound highly suspicious and easy to recognize as a scam (which might explain why it was posted online as a scam).

In the *political robocall* samples, the typical content is a prerecorded message making a political advertisement, or a poll asking the recipient about their political opinion. In the United States, political robocalls are exempt from regulation by the national Do-Not-Call Registry and the Telephone Consumer Protection Act of 1991. Before a national or state level election, they are distributed in high frequency using voice and voicemail broadcasting autodialers. All of the audio samples contained a prerecorded message, and most polls used an IVR system to interact with the recipient.

3) Mass Distribution: Mass distribution is the next critical step to a successful spam operation. The goal is to massively and cost-effectively deliver the spam content to a list of telephone numbers.

Using VoIP service to distribute calls to PSTN numbers, the content can be disseminated at a much higher volume, and at a fraction of the cost compared to traditional telephony. To understand the distribution cost of spamming, we researched the prices and found hundreds of VoIP service providers offering pay-by-the-minute calling service to US telephone numbers priced around $0.01 per minute. We also found some fixed monthly-fee pricing model with unlimited calling for about $150, however, these service providers tend to target small businesses, and these plans usually come with throttling, so high volume calling services are almost always offered with a pay-by-the-minute model.

Some VoIP service providers (such as CallFire[1] and Call-Em-All[2]) even cater specifically to telemarketers, providing features such as integrated autodialer and customizable caller ID in their service.

4) Circumvention: Spamming is an adversarial game, as spam defenses are widely introduced, the spammer has an incentive to defeat them. According to a poll conducted by Harris Poll on behalf of WhitePages in 2013, 22% of US smartphone users used a call-blocking app or a feature to block calls on their device [12]. Most mobile phones today contain basic capability to automatically block calls from a list of unwanted callers.

For the spammers today, two common ways to defeat them is to use voicemail injection and caller ID spoofing.

Voicemail injection is a recent extension of the autodialer which delivers prerecorded voice messages into the recipients' voice mailbox (voicemail). Typically, when a phone call is unanswered or declined, it gets forwarded to an answering machine that lets the caller leave a voice message. A voicemail broadcasting autodialer uses Answering Machine Detection (AMD) [13] technology to automatically complete the process of inserting a prerecorded voice message into the recipient's voicemail. A more recent type of voicemail broadcaster can even deliberately trigger the recipient's voicemail, a technique known as Forced Busy Channel [14], to directly inject a voice message into the recipient's voicemail without waiting for the call to be unanswered or declined.

Caller ID spoofing is the practice of deliberately falsifying the caller ID information sent to the recipient that identifies the caller of a phone call. It is particularly effective for defeating the call blockers and helps to further a variety of scams. The caller ID service provides the caller's telephone number (and in some cases the caller's name) to the recipient before or during the ring of an incoming call. It allows the recipient to decide whether to answer a call based on the caller ID information, or to call back if the call could not be answered. The caller ID number is also widely used in other non-voice communication services, such as SMS, MMS, and many smartphone apps. The caller ID number is typically provided by the caller's switch, which can control what caller ID number is sent on a call-by-call basis. For general consumers, a legally mandated privacy feature allows them to hide the calling number [15]. However, malicious callers can also take advantage of the declarative nature of the caller ID mechanism to spoof or block the caller ID number, in order to defeat spam filters and further a variety of scams. The caller ID number can be easily spoofed because there is no built-in authentication mechanism, and it is not immediately verifiable by the recipient. The caller's service provider does not have any legal obligation to ensure that the caller ID number in the call request header is indeed owned by the caller before it is transmitted. In fact, some ITSPs today advertise customizable caller ID as a service feature.

III. Key Challenges

We identify several challenges in combating telephone spam—that are significantly different from email spam—some of which are technical and some of which are regulatory.

[1]https://www.callfire.com/

[2]https://www.call-em-all.com/

A. Immediacy Constraint

Unlike email, which can be queued for later analysis, a voice call has an immediacy constraint. A telephone call request is immediate and therefore must be analyzed as soon as it appears, and the telephone anti-spam system must complete analysis and take action within a short window of time to reduce the delay. If a solution adds too much delay to a call request, the legitimate caller may assume that the recipient could not answer the phone and hang up.

B. Difficulty of Working with Audio Streams

The content of a voice call is difficult to parse and analyze: the content is an audio stream as opposed to the text of an email. To make matters worse, the content of a voice call is only revealed when the call is answered, and both the caller and the recipient will be affected if an anti-spam system answers the call. Whereas an email anti-spam system can easily analyze the content of an email, and neither the sender nor the receiver is affected.

C. Lack of Useful Header Data

Voice calls lack the rich header data of email. When a call arrives at the recipient, it contains little useful header information. An example of a call header used in traditional phone terminals is shown in Table III in the Appendix. An email header, however, has well-defined and information-rich SMTP headers—before the content of the email. It is also difficult to omit the sender's IP address and domain name of the email. This is in stark contrast to a call request header, where the header data is easily omittable by a spammer.

D. Hard to Gain User Acceptance

The bar for user acceptance of a telephone anti-spam system is much higher compared to email. Consumers, rightly, have a very low tolerance for false positives of blocked calls. Phone calls tends to be more urgent and important compared the email, and once a phone call is wrongfully blocked it could have severe consequences.

E. Caller ID Spoofing

The *Caller ID* service is an information service that provides the recipient with information of the caller before answering the phone, which could be useful for blocking spam calls. However, caller ID fundamentally has no authentication mechanism and is easily spoofed. The only security mechanism comes from having the TSP send the caller ID on behalf of the caller. This security mechanism is eroded when the spammer subscribes to a TSP service that allows customization of caller IDs. It used to be prohibitively expensive for individuals and small businesses to purchase the equipment necessary to enable the customization of caller IDs (an ISDN-PRI trunk line costs $500 to more than $1,000 per month and a PBX system that costs thousands [16]). With the rise of VoIP services that provide features such as caller ID customization over the Internet, it is trivial for any caller to cheaply and effectively spoof the caller ID. Thus, any telephone spam defense technique that relies on the caller ID is now vulnerable to caller ID spoofing.

F. Difficulty of Tracing Spam Calls

One way to combat spam is to make it illegal and enforce those laws. In the history of email spam, a small number of players were responsible for the majority of the spam, hence taking action against these big targets resulted in significant drops of spam volume. For instance, shutting down the Rustock botnet reduced global spam levels by around 40% [17]. It is reasonable to assume a similar distribution of telephone spammers. Unfortunately, identifying the actual distribution of telephone spammers is difficult due to the technical and regulatory challenges of monitoring PSTN traffic and the prevalence of caller ID spoofing.

It is difficult to locate the true origin of a call after it has been initiated. PSTN calls are designed to work on the principle of forwarding tables and circuit switching. Each time a call is placed, only the destination number is used for routing. It works by establishing individual circuits down a sequence of neighboring switches until it ends up at the recipient's terminal. The outbound switch(es) do not necessarily need to know whether the optional caller ID number in the call request header would route back to the caller's terminal. If the outbound switch also serves as the caller's inbound switch, then the TSP could perhaps verify the true owner of the caller ID number from its own records. However, the TSPs do not have a legal obligation to perform any verification, or to share that information with the recipient, thus, without the cooperation of the caller's TSP, tracing a spam call is almost impossible.

To make matters worse, as spam calls can now be initiated over the Internet, a spammer can further hide behind proxies, VPNs, or Tor networks, or even distribute outbound calls using a botnet, adding even more difficulty in tracing the exact whereabouts of a spammer.

G. Entrenched Legacy Systems

The PSTN ecosystem has been around for several decades, allowing any phone to reach any other phone through a vast interconnection of switching centers. While the core networks have evolved to be almost entirely carried by an IP-based infrastructure, the signaling protocols have not changed (to ensure legacy compatibility). Even though VoIP is touted as a major revolution of voice communication, the legacy of PSTN protocols will remain for many years to come. Change is difficult when the entire ecosystem must ensure that the majority of legacy systems will work, and therefore wholesale replacement of the core telephony system is a nonstarter. As a result, telephone spammers can exploit the weaknesses in the legacy technology (such as the

lack of caller ID verification) to run a successful spamming operation.

H. Lack of Effective Regulations

Unfortunately, there is also a lack of incentive for the industry to participate in the anti-spam effort. Unlike email and Internet traffic where the peering model [9] incentivizes the Internet service providers to reduce the load of spam traffic on their systems, telephony service providers profit from the spam-generated traffic and intercarrier compensation fees. Most players (phone number collectors, lead sellers, telephony service providers, and backbone carriers) in the PSTN ecosystem profit from telephone spam, except the consumer. Although TSPs may benefit in other ways by reducing telephone spam (for instance, in better public relations or charging spam-filtering service as a fee), there exists, at least, a minor monetary disincentive.

Further complicating matters, the current United States law ensure that TSPs are immune from liability for servicing spam calls [18] under the Telephone Consumer Protection Act of 1991, which means that they cannot be held liable for servicing spam calls. Classified as common carriers, *TSPs have an obligation to move all phone traffic with no exceptions* [19]. Therefore, it is difficult to implement anti-spam solutions at the most natural place: the TSP who has a direct view of the telephony network.

I. Lack of Globalized Enforcement

In the United States, a number of laws and regulation exist at both the federal and state levels, such as making robocalling illegal (with some exemptions) [20], making caller ID spoofing illegal (with some exemptions) [21], and the establishment of a national Do-Not-Call Registry [22]. The FTC is also interested in stopping telephone spam, and they have held numerous competitions to combat robocalling [23]. Despite resolute efforts by the US government, robocalling and caller ID spoofing is still an unsolved problem. Technology and globalization have resulted in *telephony networks shifting from a national ecosystem to a global ecosystem*. With the use of VoIP service, a telephone spammer can cheaply distribute outbound calls from an overseas location. Because the spammers lie beyond the jurisdiction of US law enforcement authorities, it is hard for law enforcement to prosecute those spammers for breaking the law. Effective control of telephone spam would therefore require cross-border enforcement. However, cross-border jurisdiction of telephone spam has yet to catch up with the present technology, and many countries would have no incentive to cooperate with US regulatory and enforcement agencies.

IV. Basic Techniques

To identify the state-of-the-art in preventing voice and voicemail spam, we gathered existing techniques from academic, industry, SPam over Internet Telephony (SPIT), and Internet domain, and systematically categorize them into the following classes: (1) Call Request Header Analysis, (2) Voice Interactive Screening, and (3) Caller Compliance.

A. Call Request Header Analysis

Call Request Header Analysis is a category of techniques that filters calls based on the header information associated with the call request. For instance, the caller ID is a popular type of request header information that can be used to analyze a call. The effectiveness of Call Request Header Analysis depends on the accuracy of the information collected, which could be severely impacted when spoofing or omission is possible.

Caller ID Blacklisting rejects a call if the caller's phone number (captured from caller ID or Automatic Number Identification service) appears on a blacklist, otherwise, calls from all other phone numbers are accepted. This can be used to block spam calls by blacklisting phone numbers that are known to be spamming, and the recipient's terminal would silently block all phone calls from those phone numbers without disturbing the recipient. Caller ID Blacklisting only blocks phone numbers that are explicitly added to a blacklist, hence it tends to be permissive to all other callers. As caller ID service has become ubiquitous in all telephone services, Caller ID Blacklisting does not face compatibility issues. Caller ID Blacklisting is easy to implement and requires very little computational resources, and it is a common feature in modern smartphones [24], [25]. However, a blacklist must be well populated to be effective against spam, therefore compiling a comprehensive list would not be scalable for the recipient. A spammer could defeat Caller ID Blacklisting by spoofing any number not known to be blacklisted, hence it is not effective against most forms of call request header manipulation.

Caller ID Whitelisting only accepts calls from phone numbers that appear on a whitelist, otherwise, calls from all other phone numbers are rejected. This can be used to block spam calls by whitelisting phone numbers that are known to be trusted, and the recipient's terminal would silently block phone calls from all other phone numbers without disturbing the recipient. Caller ID Whitelisting is easy to implement and requires very little resources, and it is easy to find implementations on modern smartphones [26], [27]. Caller ID Whitelisting blocks all calls that are not added to a whitelist, and does not need to be well populated to be effective against spam, hence it is quite scalable for the recipient when defending against spam. It is usually quite easy to populate a whitelist, as the numbers could be derived from the recipient's contacts list. However, unknown legitimate callers would always get blocked in Caller ID Whitelisting. A spammer could defeat Caller ID Whitelisting by spoofing the caller ID of a number known

to be trusted by the recipient, however this is more difficult without prior knowledge about the recipient's whitelist.

Caller Reputation System uses reputation or trust associated with a caller's phone number to determine if the caller is a spammer. A Caller Reputation System maintains and publishes reputation scores associated with individual callers, in which the reputation scores are computed based on various caller-related information such as recipient black/white-lists [28]–[31], caller behavior [29], [32], [33], recipient behavior [28], [34], [35], caller's domain reputation [30], [36], social connections [34], [37]–[40], and recipient feedbacks [28], [29], [31], [36], [41], [42]. There are also many opportunities to improve a Caller Reputation System by developing better scoring algorithms. The Caller Reputation System can be used to filter spam calls by configuring the recipient's terminal to block calls from callers associated with poor reputation. A Caller Reputation System generally requires a large amount of data, which are usually crowdsourced from many recipients, and the data would need to be curated by an administrative third party. It would also require frequent maintenance to ensure quality and freshness of data in order to be effective. However, large scale collection of personal information could be at risk of violating privacy. Caller Reputation System could be vulnerable to Sybil attacks, where a malicious caller obtains multiple identities to gain a large influence over its own (or other caller's) reputation. Because the reputation of a caller is associated with the caller's phone number, a spammer could defeat the Caller Reputation System by spoofing the caller ID to a number with a good reputation. A malicious caller could also sabotage someone by deliberately making junk calls while spoofing the caller ID number, such that the victim gets a poor reputation.

Caller Behavior Analysis uses the call behavioral features associated with a caller's phone number to determine if the caller is a spammer, using behavioral features such as call count/velocity [29], [33], [39], [43]–[49], call duration sum/mean/variance [29], [39], [44]–[46], [48]–[50], call rejection count/ratio [35], [39], [44], [46], [47], [49], [51], [52], recipient diversity count/ratio [44], [45], [49], [52], invalid recipient count/ratio [39], [47]–[49], [51], repeated call count/ratio [45], [52], outbound-to-inbound ratio [33], [48], [51], [53], [54], simultaneous calls [46], and caller's domain behavior [32], [51]. There are also many opportunities to improve the technique by developing better classification algorithms. Acquiring the caller's behavioral information usually requires participation from the caller's telephony service provider or a honeypot of telephones [33], [35]. If not required by regulation, it is usually not in the TSP's business interest to report on or impose a call behavior restriction on their callers. The callers' behavioral information would need to be updated frequently to ensure accuracy and freshness in order to be effective. Large scale collection of callers' call behavior could also face privacy issues and numerous obstacles from legal regulations. Because the call behavior of a caller is associated with the caller's phone number, a spammer could defeat the Caller Reputation System by spoofing the caller ID to a number with good calling behavior. Furthermore, a spammer could hide its illegitimate call behaviors by using multiple caller identities.

Device Fingerprinting collects a variety of metadata from the call request header for the purpose of creating a device fingerprint of a caller's terminal. Device fingerprinting improves the accuracy of determining the caller's identity by using only a set of information that meets the properties of diversity and stability. Device Fingerprinting has been proposed for SPIT prevention by blacklisting or whitelisting the device fingerprints of SIP-based terminals [55]. However, in PSTN, device fingerprint information is a scarce resource. This is due to the little amount of header information in PSTN call requests (an example of which is shown in Table III in the Appendix) compared to SIP or email, resulting in having too little workable information for device fingerprinting to work effectively.

Caller ID Anomaly Detection searches for anomalous patterns in the caller ID, such as invalid format, invalid number, unavailable number, toll-free number, area codes, regular expression, to determine if the caller is a spammer. Caller ID Anomaly Detection is quite easy to implement and requires very little computational resources and, therefore, is easy to find in several call blocking apps [56], [57]. Caller ID Anomaly Detection does not track information associated with any individual caller, instead, it looks for general patterns in the caller ID that can be used to differentiate spammers and legitimate callers. As Caller ID Anomaly Detection tend to find matches more broadly, it tends to be easier to manage and maintain. However, some patterns may be potentially prone to false negatives, and therefore may restrict some legitimate callers, such as VoIP users or privacy enabled callers. A spammer could defeat Caller ID Anomaly Detection by carefully crafting the caller ID to not trigger any known anomalous patterns.

ANI-CPN Matching checks whether the Calling Party Number (CPN) captured by the caller ID service matches with the Automatic Number Identification (ANI) number captured by the ANI service [58]. Automatic Number Identification service [59] is a separate type of calling line identification service that can capture the calling number information even when the caller ID is not presented. It was originally designed to obtain the calling party's billing number from a local exchange carrier to any interconnecting carrier for billing of long distance calls. In most cases,

the billing number is the same as the CPN, and usually when a mismatch happens it is likely due to caller ID spoofing, or the caller is calling from a private branch exchange (PBX). ANI-CPN Matching assumes that a legitimate caller's CPN matches the ANI number whereas a malicious caller would spoof the CPN which results in a mismatch. However, ANI service are usually not made available to regular consumers (usually only offered to 800 toll-free, 900 premium-rate, or 911 emergency service lines), therefore, only some businesses would benefit from this technique. ANI service is also not always reliable at capturing the caller's ANI number. Placing a legitimate call using an outbound VoIP service or a calling card service would result in a non-working or a generic ANI number being captured. As a result, false positives may frequently occur which hinders user acceptance.

ANI-II Filtering can be used to filter spam calls by blocking certain types of origin service captured by the ANI-II service. ANI-II [60] is an extension of the ANI service that identifies the type of service associated with the originating switch. Each type of service is represented by a two-digit code. ANI-II Filtering assumes that legitimate callers would have a valid (00 or 61) ANI-II code, whereas, malicious callers would be making VoIP calls that would have an invalid ANI Failure (02) code, and therefore should be blocked. However, with the growing use of VoIP service by regular consumers, this technique could potentially result in too many false positives if all calls with ANI Failure codes are blocked. Only some businesses would benefit from an implementation of this technique, as ANI-II service is usually offered only to premium-rate, toll-free, or emergency lines. Therefore, this technique would not be accessible or cost effective for the regular consumers.

B. Voice Interactive Screening

Voice Interactive Screening is a category of techniques that forces the caller to interact with a voice input-based interactive system and decide if the call is spam after analyzing the caller's interaction. The system either requires active or passive interaction from the caller. An active interaction system relies on the caller providing a response to a specific task which requires some effort from the caller, whereas a passive interaction system silently gathers the caller's response without explicitly informing the caller. Voice Interactive Screening techniques do not need to rely on the caller ID or any other call request header information, hence they are generally not vulnerable to caller ID spoofing. However, Voice Interactive Screening techniques generally require processing of audio signals, which tends to be more complex to implement. Because these techniques can only work *after* recording a length of the caller's voice, all Voice Interactive Screening techniques have a screening period, therefore, would introduce additional delay to the caller. Due to the recording of the caller's voice during the screening, in the US, some states require explicit consent of recording the conversation, which could hinder the screening process or invoke privacy fears from some legitimate callers. As telephone audio can be manipulated, and tends to contain artifacts such as background noise, network dropouts, or compression losses, Voice Interactive Screening techniques are generally more prone to errors.

Audio Fingerprinting uses the voice recording of the caller, or audio features extracted from the voice recording of the caller, to analyze for similarity to a set of known spam call profiles. If the voice recording is similar to an audio stream of a known spam profile, then the call is classified as spam. Audio Fingerprinting has been proposed to combat replayed voice spam in several works [61]–[67]. However, the performance of Audio Fingerprinting depends on the completeness of spam profiles, which is usually not feasible for a recipient to collect. Audio Fingerprinting would usually require a thirty-party to continuously collect and maintain the known-spam audio profiles to ensure effectiveness. However, a spammer could potentially defeat the mechanism by dynamically creating variations of the spam audio message (such as adding audio artifacts or using personalized messages) to avoid identification.

Speech Content Analysis first records the caller's voice, then makes use of speech recognition technology to transcribe the voice into text. The text is then analyzed with text profiles of known spam calls to classify if the call is spam. As opposed to managing audio recordings, a corpus of text data is usually much easier to manage. As many spam calls are simply variations of a call script, a keywords-based classification model could be used against variations of a same type of spam [68]. However, the effectiveness of this technique depends on the accuracy of speech recognition, and of course the effectiveness of the classification model. In practice, automatic speech recognition of telephone voice is an ongoing research problem [69], which tends to be prone to errors, and still has several years to go to reach human-level performance [70].

Acoustic Pattern Analysis extracts distinguishing acoustic patterns from the caller's audio stream, such as signal losses [71], peak uniformity [71], noise uniformity [71], voice activity [72], [73], and double talks [72]–[74], to determine if the call is spam. Audio Fingerprinting looks for general patterns in the audio signal that can broadly distinguish spam calls from legitimate calls. Unlike Audio Fingerprinting and Speech Content Analysis, Acoustic Pattern Analysis does not require a large collection of known-spam profiles, which could be difficult to gather and

maintain. However, some patterns may be prone to false positives and could be easily defeated with manipulation of the audio stream.

CAPTCHA/Turing Test is an interactive challenge-response technique that requires the caller to complete a reverse Turing test to determine whether the caller is a human or robocaller. The tests are designed to be difficult for a computer but easy for a human to complete. For instance, the test could ask the caller to key in what they hear from a distorted audio stream of random numbers [75]–[77]. However, CAPTCHA/Turing Test would need to be careful not to discriminate against certain groups of people, such as people with poor English or disabilities, while not giving too much leeway for abuse by "decaptcha" systems [78]. On the other hand, CAPTCHA/Turing Test would also need to be careful not to be illegible even for users with no handicaps, as the legitimate caller may become irritated by the obstacles of initiating a call with the recipient. Because CAPTCHA/Turing Test is highly interactive, it tends to require a high degree of effort, and cause significant delays to the caller.

C. Caller Compliance

Caller Compliance is a category of techniques that require the caller to first satisfy a compliance requirement prior to or during a call request. If the caller is able to satisfy the compliance requirement, then the caller is allowed to communicate with the recipient. Satisfying the requirements should be easy for a legitimate caller but difficult (or costly) for a spammer. Some compliance measures require special changes made to the call setup process or to the communicating terminals. Some techniques require prior instructions given to the caller.

Do Not Call Registry simply provides a registry of phone numbers that spammers are legally prohibited from calling in most circumstances. The spammer may be subject to substantial fines if they fail to comply. The registry is usually maintained by the national government, in the US [22], the list is maintained by the Federal Trade Commission. However, the recipients would need to actively provide feedbacks for the government to legally act on spammers violating the law. The Do Not Call Registry can act as a good deterrence for domestic law-abiding telemarketers, however it would have little effectiveness on spoofed numbers and overseas spammers.

Graylisting [79] first rejects the initial call request from a caller and then accepts the next call request from the same caller made within a short period of time. This technique defends against autodialers that simply call a list of phone numbers and do not make repeated call attempts. The technique also assumes that if an uninformed (about the defense) caller is calling about legitimate business, the caller will try again. The implementation is simple and does not require changes to the infrastructure. However, the legitimate caller must make two calls for every call request, which introduces additional delay and calling cost. A spammer could easily defeat the Graylisting mechanism by configuring the autodialer to automatically call again if a call goes unanswered, but at the cost of higher phone bills and reduced efficiency.

Consent-based Communication first requires the caller to send a consent request to the recipient before initiating a call. For instance, the request could be a forwarded greeting message where an answering machine first records the name spoken with the caller's voice and then plays it to the recipient [80]–[82]. The recipient then decides whether to accept the caller's request to communicate. If the call is spam, the recipient is only limited to being exposed to an abridged recording (or the request message) of the spam call. However, the recipient is still disturbed for every unconsented caller, therefore it is not scalable, and the recipient is not spared from the disturbance of a spam call. It also adds delay to each call, as legitimate callers are forced to wait for consent before each call.

Call Back Verification first rejects an initial call from a caller, then forces the caller to wait for the recipient to call back the caller. Call Back Verification is a good defense against caller ID spoofing, as it forces the caller to provide a genuine caller ID. The basic mechanism is simple, and some implementations try to automate this process [83], [84]. However, it requires the caller to first own a reachable inbound number, which could restrict communication from legitimate VoIP users and telephone extension terminals. Call Back Verification also add delays to each communication, as the legitimate caller must wait for the recipient to call back. Calling back could also add calling cost on both the caller and recipient in PSTN, which can be especially significant for premium or international numbers.

Weakly Secret Information requires the caller to demonstrate knowledge of a weakly secret information before allowing communication with the recipient. Weakly secret information could be in various forms such as a passcode, an extension code, a limited-use phone number, or a message identifier [85]. However, the recipient would first need to share the weakly secret information to all trusted callers, hence it may not be scalable for a recipient with a large contact list. Legitimate calls from unknown callers would also be restricted from communicating with the recipient.

Payment at Risk is a micropayment, cost-based, technique where the caller is required to deposit a small amount of money before making a call. If the recipient reports that the call is spam, then the deposit is confiscated or kept by the recipient, otherwise the money is refunded to the caller. This was proposed as a method for SIP spam prevention [38]. This technique prevents spamming by making it prohibitively expensive to send out a large amount of spam calls, while costing very little for legitimate callers. However, the solution requires a universal micropayment system that collects payment on every call, which may require significant resources to create and administer. There also are many questions regarding the legality of this approach, for instance on the lawful confiscation of payments and abuse of spam reporting. The value amount of the deposit would also affect the number of recipients needed to report on the spam caller to effectively make spamming unprofitable.

Proof of Work is a computational, cost-based, technique where the caller's terminal is required to produce a proof-of-work, such as hashcash [86], that is moderately hard to compute (being computational or memory-bound) but easy for the recipient to verify, before allowing communication with the recipient. As the amount of work increases, it would be prohibitively inefficient to distribute large amounts of spam calls. A legitimate caller would not be significantly affected for making a few number of calls. On one hand, Proof of Work has an advantage over Payment at Risk by not requiring a micropayment system, therefore avoiding the administrative and legality issues. On the other hand, Proof of Work faces a trade-off problem between permissiveness and anti-spam effectiveness. In PSTN, due to the significant share of low-end telephone terminals, the difficulty of the work would need to be low enough to ensure permissiveness. However, this may allow a spammer using moderately powerful computerized terminals to easily generate as much work as needed for spamming. Legitimate callers with high outbound calls, such as a bank, may also be obstructed from doing legitimate business if it is prohibitively costly to generate the proof-of-works to contact a large number of customers.

Proof of Identity requires the caller to send a verifiable identity token that would authenticate the credentials of the caller whenever making a call. This technique has been proposed for SIP domain users [83], [87]–[89], due to the availability of SSL/TLS certificates and maturity of the underlying public key infrastructure. This technique prevents spamming by ensuring that the caller could be held responsible for making illegal calls, and prevents scams by ensuring that the caller cannot impersonate as someone else. Proof of Identity could also prevent a spammer from using multiple identities when identity verification is required. Proof of Identity has an advantage over Proof of Work by not having the issue of deciding the right difficulty level of proof-of-work which could either obstruct calls from low-end telephone terminals or give too much leeway for spamming. However, the scheme could be hard to deploy in PSTN, as it would require establishment of a certificate authority for issuing and verifying caller identities, and may require significant changes to the call request protocols in PSTN.

V. Assessment Criteria

It is clear that there is no shortage of techniques to combat telephone spam, but what would an ideal telephone spam defense entail? Therefore, we propose a set of assessment criteria.

We separate the assessment criteria into three categories: (1) Usability, which evaluates the ease-of-use from either the caller or recipient's perspective, (2) Deployability, which evaluates the ease of installation, deployment, and operation, and (3) Robustness, which evaluates the technique's resilience against errors and effectiveness against a spammer actively evading the defense. We define each of the identified criteria and give a mnemonic name.

A. Usability Criteria

No-Disturbance-to-Recipient When a known-spam call arrives, the technique does not disturb the recipient, such as prompting for additional action from the recipient.

Scalable-for-Recipient The technique does not increase the burden of work on the recipient with an increasing number of spam calls. The technique can handle a large variety of spam calls with minimal input from the recipient.

Effortless-for-Caller When initiating a call, the technique requires minimal or zero effort from the caller.

Negligible-Changes-to-Call-Setups The technique requires negligible changes to the existing call setups or configurations in the callers' terminals.

Negligible-Delays When initiating a call, the technique adds negligible or unperceivable delay to the caller, other than the typical time to connect and time waiting for the recipient to answer the phone.

Permissive-for-VoIP-Callers The technique would not restrict any legitimate calls that use VoIP service. For instance, some outbound-only VoIP users (such as Skype) tend to have a generic (or unavailable) caller ID number and cannot receive incoming PSTN calls.

Permissive-for-Unknown-Callers The technique would not restrict calls from a legitimate caller not known by the recipient.

B. Deployability Criteria

Negligible-Changes-to-Infrastructure The technique requires zero or negligible changes to existing PSTN protocols, terminals, or infrastructure.

No-Third-Party-Involvement The technique does not require a third-party. A compromise of the third-party would not result in mishandled calls or in a breach of privacy.

Low-Resource-Requirement The technique is lightweight and does not require a significant amount of resources (e.g., people, equipment, engineering, or funding) to initiate and deploy.

Low-Maintenance The technique requires low maintenance, in terms of administrative cost, time, or resources, to maintain good working order.

Negligible-Cost-per-Call The technique adds negligible cost to each call, taxed on the legitimate caller, recipient, third-party, or carriers. The cost could also be indirect, such as reduced efficiency or capacity.

C. Robustness Criteria

Effective-Against-Dynamic-Caller-ID-Spoofing The technique is robust even when the spammer spoofs different caller IDs nondeterministically.

Effective-Against-Targeted-Caller-ID-Spoofing The technique is robust even when the spammer spoofs a specific caller ID known to be trusted by the recipient.

Effective-Against-Unavailable-Caller-ID The technique is robust even when the spammer makes the caller ID unavailable or sends a faulty caller ID to cause errors.

Effective-Against-Multiple-Identities The technique is robust even when the spammer initiate calls from multiple sources, such as using multiple subscriber accounts or a telephone botnet, to disseminate spam calls. This is different from caller ID spoofing where the caller IDs are not necessarily spoofed but are instead initiated from different sources.

Effective-Against-Answering-Machine-Detection The technique is robust even when the spammer uses Answering Machine Detection technology, which is a feature in autodialers that can distinguish human pick-ups from answering machines. With AMD, an autodialer can be configured to call again later if the call was not answered by a human, or to deliver the audio message into the recipient's voicemail.

Effective-Against-Dynamic-Audio-Content The technique is robust even when the spammer uses an autodialer capable of personalizing or altering the audio messages for different recipients. This is usually featured in autodialers that are able to synthesize text to speech.

We evaluate each technique using the criteria proposed in Section V, and Table I visually summarizes this evaluation. Each technique is evaluated as either satisfying the criteria (denoted as ●), may satisfy the criteria (denoted as ◐), or not satisfying the criteria (denoted as ○). "May satisfy the criteria" means that the technique can be made to satisfy the criteria depending on the implementation or configuration, while some implementations do not fully satisfy the criteria.

Of course, this analysis requires some opinion, and in each case we evaluated each technique and criteria to the best of our abilities. While others may disagree with the exact assessment of each technique, we believe that the criteria outlined in Section V will help to guide future telephone spam defenses and to provide a framework to evaluate these defenses.

VI. Combining Techniques

From analyzing all the standalone techniques, it is clear that there is no single technique that can satisfy all the criteria. Therefore, an improved anti-spam system would look to combine different techniques, to leverage the positives and compensate the negatives. We outline the different ways in which a solution could use a combination of standalone techniques.

Phased Decisions combine several techniques into a linear sequence (i.e., a pipeline process) of decision stages. If an earlier technique determines the call is spam, then it may not be necessary to run the evaluation techniques at later stages. This is suitable for combining techniques that uses information that are obtained chronologically, such as first using Call Request Header Analysis, followed by Voice Interactive Screening. We found use of Phased Decisions approach in related works by Niccolini and Quitek et al. [96], [97], Schlegel et al. [98], Gritzalis and Mallios [99], [100], and Azad and Morla [39].

Weighted Scoring combines several techniques by running each technique individually and then combining the outputs to produce a final score by applying a weighted scoring method. The classification of whether the call is spam is based on the final score. As Weighted Scoring need to collect outputs from all standalone techniques, it is suitable for combining techniques that can be performed

		References	Usability						Deployability						Robustness					
			No-Disturbance-to-Recipient	*Scalable-for-Recipient*	*Effortless-for-Caller*	*Negligible-Delays*	*Permissive-for-VoIP-Callers*	*Permissive-for-Unknown-Callers*	*Negligible-Changes-to-Infrastructure*	*Negligible-Changes-to-Call-Setups*	*No-Third-Party-Involvement*	*Low-Maintenance*	*Low-Resource-Requirement*	*Negligible-Cost-per-Call*	*Effective-Against-Dynamic-Caller-ID-Spoofing*	*Effective-Against-Targeted-Caller-ID-Spoofing*	*Effective-Against-Unavailable-Caller-ID*	*Effective-Against-Multiple-Identities*	*Effective-Against-Answering-Machine-Detection*	*Effective-Against-Dynamic-Audio-Content*
Call Request Header Analysis	Caller ID Blacklisting	[24], [25]	●	◐	●	●	●	●	●	●	●	◐	●	●	○	○	○	◐	●	●
	Caller ID Whitelisting	[26], [27]	●	●	●	●	●	○	●	●	●	◐	●	●	●	○	○	●	●	●
	Caller Reputation System	[28]–[42], [90]	●	◐	●	●	●	◐	●	●	◐	○	◐	●	◐	○	○	◐	●	●
	Caller Behavior Analysis	[29], [32], [33], [35], [39], [41], [43]–[54], [91], [92]	●	●	●	●	●	◐	●	●	◐	○	◐	●	◐	○	○	◐	●	●
	Device Fingerprinting	[55]	●	●	●	●	●	◐	●	●	◐	○	◐	●	◐	○	◐	◐	●	●
	Caller ID Anomaly Detection	[56], [57]	●	●	●	●	●	●	●	●	◐	◐	●	●	◐	○	◐	○	●	●
	ANI-CPN Matching	[58]	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	○	◐	○	●	●
	ANI-II Filtering	[58]	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	○	◐	○	●	●
Voice Interactive Screening	Audio Fingerprinting	[61]–[67]	●	●	◐	○	●	●	●	●	◐	○	○	◐	●	●	●	●	◐	◐
	Speech Content Analysis	[62], [68]	●	●	◐	○	●	●	●	●	◐	◐	○	◐	●	●	●	●	◐	◐
	Acoustic Pattern Analysis	[71]–[74]	●	●	◐	○	●	●	●	●	◐	◐	◐	◐	●	●	●	●	◐	◐
	CAPTCHA/Turing Test	[75]–[77]	●	●	○	○	●	●	●	●	●	◐	◐	◐	●	●	●	●	●	●
Caller Compliance	Do Not Call Registry	[22]	◐	◐	◐	●	●	●	●	●	○	◐	◐	●	○	○	○	◐	●	●
	Graylisting	[74], [79]	●	●	◐	○	●	◐	●	◐	●	●	●	○	●	●	●	●	●	●
	Consent-based Communication	[80]–[82]	○	○	◐	○	●	◐	●	◐	●	●	●	◐	●	◐	●	●	●	●
	Call Back Verification	[83], [84]	◐	◐	◐	○	◐	◐	●	●	●	●	●	○	●	●	●	●	●	●
	Weakly Secret Information	[85]	●	◐	◐	◐	●	○	◐	◐	●	◐	●	●	●	●	●	●	●	●
	Payment at Risk	[38]	●	○	◐	●	●	○	○	○	○	○	○	○	●	●	●	●	●	●
	Proof of Work	[86], [93]–[95]	●	●	●	●	●	○	◐	○	●	●	◐	●	●	●	●	●	●	●
	Proof of Identity	[83], [87]–[89]	●	●	●	●	●	○	◐	○	◐	●	◐	●	●	●	●	●	●	●

●= satisfy the criteria ◐= may satisfy the criteria ○= does not satisfy the criteria

Table I: Evaluation of various standalone techniques against the criteria described in Section V.

simultaneously, such as the various standalone Call Request Header Analysis techniques. We found use of Weighted Scoring approach in related works by Dantu and Kolan [101], Niccolini and Quitek et al. [96], [97], Schlegel et al. [98], Hansen et al. [102], and Mathieu et al. [103].

Conditional Procedures combine several techniques based on a predefined set of rules (i.e., a policy or an algorithm). This allows for higher flexibility of combining the techniques, such as using a different sequence of standalone techniques based on the preference of each recipient or the reputation of each caller. We found use of Conditional Procedures approach in related works by d'Heureuse et al. [104], Dritsas et al. [105], Scata and La Corte [106], and Soupionis and Gritzalis [47].

We evaluate existing solutions using a combined approach, and summarized which standalone techniques those solutions incorporated in Table II. All of these works are mainly focused on defense against SPIT, and some of these may include SPIT-specific techniques that does not appear in our table. Again, this analysis requires some opinion, and we evaluated each solution to the best of our abilities. We believe that the various strategies of combining techniques outlined in Section VI will help to improve future telephone spam defenses.

VII. Related Work

While in this paper we have compared and analyzed the state-of-the-art research in telephone spam defense, we will now discuss related survey papers. Most of the papers focus on spam in the Voice over IP (VoIP) domain, so-called SPam over Internet Telephony (SPIT), rather than the larger PSTN telephony network.

Keromytis [107], [108] presented two comprehensive surveys of VoIP security, which summarized previous works related to VoIP security and organized them according to an extended version of the VoIP Security Alliance (VoIPSA) Threat Taxonomy. The papers reviewed many previous works addressing every type VoIP threat in the VoIPSA taxonomy, with the social threats of spamming as one of the categories.

	[96], [97]	[98]	[99]	[100]	[101]	[102]	[103]	[104]	[105]	[106]
Phased Decisions	✓	✓	✓	✓						✓
Weighted Scoring	✓	✓			✓	✓	✓	✓		
Conditional Procedures								✓	✓	✓
Caller ID Blacklisting	✓	✓	✓	✓	✓	✓	✓		✓	✓
Caller ID Whitelisting	✓	✓		✓	✓	✓	✓		✓	
Caller Reputation System	✓		✓	✓	✓	✓			✓	✓
Caller Behavior Analysis	✓	✓	✓		✓	✓	✓		✓	✓
Device Fingerprinting										✓
Caller ID Anomaly Detection										
ANI-CPN Matching										
ANI-II Filtering										
Audio Fingerprinting				✓						
Speech Content Analysis	✓									✓
Acoustic Pattern Analysis	✓									
CAPTCHA/Turing Test	✓	✓	✓	✓		✓		✓		✓
Do Not Call Registry										
Graylisting	✓					✓	✓			✓
Consent-based Communication	✓		✓							✓
Call Back Verification										
Weakly Secret Information	✓									
Payment at Risk										
Proof of Work	✓							✓		
Proof of Identity			✓	✓					✓	

Table II: Summary of various anti-spam solutions using a combination of standalone techniques.

Baumann et al. [109] presented a survey of potential solutions to SPIT. The paper provided an overview and classification of SPIT prevention methods based on detection using Signaling versus Voice and order-based Before Call versus After/While Call. The paper also proposed a Biometric Framework for SPIT Prevention as a way to bind identities to each caller.

Phithakkitnukoon et al. [110] presented a survey focused on five primary types of VoIP attacks, SPIT being one of them. The authorized provided an introduction to the basic knowledge of VoIP systems and its available security tools, and summarized a list of proposed solutions for SPIT from previous literature.

Quinten et al. [111] presented a survey evaluating the techniques to prevent and reduce SPIT. The authors evaluated the effectiveness of techniques by dividing them into four categories: unsuitable techniques, techniques with potential, suitable techniques, and combinations of techniques.

Dantu et al. [112] presented a survey discussing the attacks and solutions in VoIP, with VoIP Spam and Phishing being one of the attacks. The authors reviewed previous work addressing all types of VoIP attacks and proposed a high-level security architecture to make the VoIP infrastructure more secure and robust.

Dritsas et al. [113] presented a survey reviewing a list of SPIT identification criteria that can be used by anti-SPIT mechanisms and identified the different detection stages. The authors propose two generic categories of SPIT identification criteria: SIP Message criteria and SIP User Agent criteria. They also proposed a two-fold evaluation framework for discovering possible SPIT messages.

Marias et al. [114] presented a survey assessing the threats and vulnerabilities that the SIP protocol introduces. The authors also reviewed existing anti-SPIT mechanisms and classified them into three classes: Prevent, Detect, and Handle. The paper also proposes a list of qualitative and quantitative criteria to assess the effectiveness of the anti-SPIT countermeasures.

Khan et al. [115] presented a survey reviewing various existing methods for preventing spam in IP telephony. The paper also presented a discussion on the implementation costs of different types of techniques, and commented that no single technique is sufficient and therefore a framework of multiple techniques is recommended.

Rosenberg et al. [116] presented an open memo reviewing various solutions that might be possible to deal with SIP spam. The author also presented some borrowed techniques that have been employed to deal with email spam. In conclusion, the author recommends using identity related techniques, while also commented that identity techniques may be vulnerable when a SIP request without an authenticated identity cannot know whether the request lacked such an identity because the originating domain didn't support it, or because a man-in-the-middle removed it.

In general, most existing survey papers focus on techniques against SPIT or more specifically spam in the SIP

protocol. This paper is focused on techniques to address spamming in the PSTN telephony network. Some techniques for SPIT are not applicable to PSTN due to protocol differences. As far as we are aware, this is the first survey paper specifically addressing spam calls directed to the PSTN telephony network. In terms of evaluation differences, we are the first to propose a taxonomy to classify the existing standalone techniques into three categories, the first to evaluate the standalone techniques based on three sets of assessment criteria, and the first to outline the three strategies of combining standalone techniques.

VIII. Conclusion

From analyzing and evaluating the existing solutions that attempt to address telephone spam, we reach the conclusion that there is no universally acceptable solution to telephone spam. Every approach thus far has different tradeoffs, specifically between usability, deployability, and robustness.

From our analysis of the telephone spam ecosystem and defensive techniques, we believe that usability is the most important criteria for evaluating a defense. Unlike email, which can be delayed or possibly lost due to a false positive, telephony solutions have a high bar for user acceptance, and we believe that users will not adopt techniques that impose excessive burden on both the caller and recipient. Therefore, future research into this area must consider the usability of the defense from both the caller and the recipient perspective.

We believe that one promising avenue of research is using a combination of techniques, which should improve on the robustness of standalone techniques, and potentially each technique could address the weaknesses of the others. However, as the telephony system has real-time immediacy constraints, care must be taken so that the combination of techniques will not degrade the user experience due to higher complexity. Our intuition leads us to recommend combining no more than two standalone techniques, as we observed that a good balance of usability, deployability, and robustness could be achieved by using two standalone techniques.

One glaring issue that continually reoccurs when analyzing the telephone spam ecosystem is caller ID spoofing. We believe that the key to combating telephone spam is to make the caller ID trusted and verifiable, while making minimal changes to existing infrastructure. For instance, from our evaluation of Call Request Header Analysis techniques, they provide the best overall usability and deployability, however they suffer from robustness due to the spammer's ability to spoof the caller ID. If caller ID spoofing can be effectively prevented, then we believe that Call Request Header Analysis would satisfy all of our evaluation criteria.

Telephone spam is poised to increase significantly, defrauding consumers of billions of dollars. Therefore, an effective telephone spam defense is critical. However, the techniques and approaches that were effective in combating email spam are inappropriate when applied to telephone spam. We attribute this to differences not only in the technology used, but more fundamentally to the type of communication. This is why a survey of the telephone spam area is necessary: to highlight these differences and to define the ideal criteria for telephone spam defenses. We hope that this paper provides a framework to help guide and shape future telephone spam defenses.

Acknowledgment

This work was partially supported by the grants from Cisco Inc. and Center for Cybersecurity and Digital Forensics at ASU.

References

[1] CTIA, "Annual Wireless Industry Survey," http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

[2] U.S. Bureau of Labor Statistics, "American time use survey fact sheet," http://www.bls.gov/tus/atussummary.pdf, June 2015.

[3] Federal Trade Commission, "National do not call registry data book fy 2014," https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2014/dncdatabookfy2014.pdf, Federal Trade Commission, Tech. Rep., 2015.

[4] Federal Trade Commission, "Consumer sentinel data book for january - december cy 2014," https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf, Federal Trade Commission, Tech. Rep., 2015.

[5] S. H. Kimball, T. Levy, H. Venturelli, and S. Miller, "Interactive Voice Recognition Communication in Electoral Politics: Exploratory Metadata Analysis," *American Behavioral Scientist*, 2014.

[6] A. R. Modarressi and R. Skoog, "Signaling System No. 7: A Tutorial," *IEEE Communications Magazine*, 1990.

[7] International Telecommunication Union, "Fixed-telephone subscriptions," http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Fixed_tel_2000-2013.xls.

[8] Statista, "Countries by number of Voice over Internet Protocol (VoIP) subscribers in 1Q 2013," http://www.statista.com/statistics/236824/number-of-voip-subscribers-by-leading-countries/.

[9] B. Woodcock and V. Adhikari, "Survey of Characteristics of Internet Carrier Interconnection Agreements," Packet Clearing House, Tech. Rep., 2011.

[10] Federal Communications Commission, "Intercarrier compensation," https://www.fcc.gov/encyclopedia/intercarrier-compensation, 2015.

[11] P. Casanova, R. Bandyopadhyay, and V. Balasubramaniyan, "Largest IRS Phone Scam Likely Exceeded 450,000 Potential Victims in March," http://www.pindropsecurity.com/irs-phone-scam-live-call_analysis/, 2015.

[12] Marketwired, "From Stalkers to Spam, WhitePages Study Breaks Down Reasons Americans Block Calls," http://www.marketwired.com/press-release/from-stalkers-to-spam-whitepages-study-breaks-down-reasons-americans-block-calls-1900134.htm.

[13] C. A. Hamilton, "Machine answer detection," Dec. 6 1994, uS Patent 5,371,787.

[14] T. Mobarak and A. Han, "Method and apparatus for forcing a call to a carrier provided voice mail facility," 2013, uS Patent 8,605,869.

[15] Federal Communications Commission, "Calling Number Identification Service–Caller ID," 2015.

[16] C. Business, "PRI Trunk Plans," http://business.comcast.com/phone/pri-trunks/plans-pricing.

[17] E. Park, "Rustock Takedown's Effect on Global Spam Volume," http://www.symantec.com/connect/blogs/rustock-takedown-s-effect-global-spam-volume, 2011.

[18] M. Carney, "Courts deem CallFire a common carrier, setting a major precedent at intersection of telecom and tech law," http://pando.com/2015/02/27/courts-deem-callfire-a-common-carrier-setting-a-major-precedent-at-intersection-of-telecom-and-tech-law/, Feb. 27, 2015.

[19] K. Cox, "FTC: Totally Fine By Us If Phone Companies Block Robocalling Numbers," http://consumerist.com/2015/01/27/ftc-totally-fine-by-us-if-phone-companies-block-robocalling-numbers/, Jan. 27, 2015.

[20] Federal Communications Commission, "Telephone consumer protection act 47 u.s.c. Âğ 227," https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf.

[21] Public Law 111âĂŞ331 111th Congress, "Truth in caller id act of 2009," https://www.congress.gov/111/plaws/publ331/PLAW-111publ331.pdf.

[22] Federal Trade Commission, "National Do Not Call Registry," https://www.donotcall.gov/.

[23] Federal Trade Commission, "Robocalls | consumer information," https://www.consumer.ftc.gov/features/feature-0025-robocalls, 2015.

[24] E. Montejo, "How to block phone calls on your Android phone," http://www.androidauthority.com/how-to-block-phone-calls-numbers-android-phone-246484/.

[25] Apple Inc., "Block calls and block or filter messages on your iPhone, iPad, or iPod touch," https://support.apple.com/en-us/HT201229.

[26] T. Nimmerjahn, "Whitelist Call Blocker," https://play.google.com/store/apps/details?id=de.tn_software.callblocker.

[27] NQ Mobile Security, "NQ Mobile Call Blocker," http://en.nq.com/callblocker.

[28] P. Kolan and R. Dantu, "Socio-technical defense against voice spamming," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 2, no. 1, p. 2, 2007.

[29] F. Wang, Y. Mo, and B. Huang, "P2p-avs: P2p based cooperative voip spam filtering," in *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. IEEE, 2007, pp. 3547–3552.

[30] P. Patankar, G. Nam, G. Kesidis, and C. R. Das, "Exploring anti-spam models in large scale voip systems," in *Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on*. IEEE, 2008, pp. 85–92.

[31] R. Zhang and A. Gurtov, "Collaborative reputation-based voice spam filtering," in *Database and Expert Systems Application, 2009. DEXA'09. 20th International Workshop on*. IEEE, 2009, pp. 33–37.

[32] C. Sorge and J. Seedorf, "A provider-level reputation system for assessing the quality of spit mitigation algorithms," in *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1–6.

[33] V. B. Payas Gupta, Bharat Srinivasan and M. Ahamad, "Phoneypot: Data-driven Understanding of Telephony Threats," in *Proceedings of the Symposium on Network and Distributed System Security (NDSS)*.

[34] P. Kolan, R. Dantu, and J. W. Cangussu, "Nuisance level of a voice call," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 5, no. 1, p. 6, 2008.

[35] T. S. Corporation, "Nomorobo," https://www.nomorobo.com.

[36] K. Srivastava and H. G. Schulzrinne, "Preventing spam for sip-based instant messages and sessions," 2004.

[37] Y. Rebahi and D. Sisalem, "Sip service providers and the spam problem," in *Proceedings of the 2nd VoIP Security Workshop*, 2005.

[38] Y. Rebahi, D. Sisalem, and T. Magedanz, "Sip spam detection," in *Digital Telecommunications,, 2006. ICDT'06. International Conference on*. IEEE, 2006, pp. 68–68.

[39] M. A. Azad and R. Morla, "Multistage spit detection in transit voip," in *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*. IEEE, 2011, pp. 1–9.

[40] M. A. Azad, R. Morla, "Caller-rep: Detecting unwanted calls with caller social strength," *Computers & Security*, vol. 39, pp. 219–236, 2013.

[41] Y.-S. Wu, S. Bagchi, N. Singh, and R. Wita, "Spam detection in voice-over-ip calls through semi-supervised clustering," in *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on*. IEEE, 2009, pp. 307–316.

[42] F. Wang, F. R. Wang, B. Huang, and L. T. Yang, "Advs: a reputation-based model on filtering spit over p2p-voip networks," *The Journal of Supercomputing*, vol. 64, no. 3, pp. 744–761, 2013.

[43] D. Shin, J. Ahn, and C. Shim, "Progressive Multi Gray-Leveling: A Voice Spam Protection Algorithm," *IEEE Network*, 2006.

[44] H.-J. Kim, M. J. Kim, Y. Kim, and H. C. Jeong, "Devs-based modeling of voip spam callersâĂŹ behavior for spit level calculation," *Simulation Modelling Practice and Theory*, vol. 17, no. 4, pp. 569–584, 2009.

[45] M.-Y. Su and C.-H. Tsai, "A prevention system for spam over internet telephony," *Appl. Math*, vol. 6, no. 2S, pp. 579S–585S, 2012.

[46] M. Amanian, M. Moghaddam, and H. Roshkhari, "New method for evaluating anti-SPIT in VoIP networks," in *Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on*. IEEE, 2013, pp. 374–379.

[47] Y. Soupionis and D. Gritzalis, "Aspf: Adaptive anti-spit policy-based framework," in *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*. IEEE, 2011, pp. 153–160, http://dx.doi.org/10.1109/ARES.2011.29.

[48] N. Chaisamran, T. Okuda, and S. Yamaguchi, "Trust-based voip spam detection based on calling behaviors and human relationships," *Information and Media Technologies*, vol. 8, no. 2, pp. 528–537, 2013.

[49] R. J. B. Chikha, T. Abbes, W. B. Chikha, and A. Bouhoula, "Behavior-based approach to detect spam over IP telephony attacks," *International Journal of Information Security*, 2015.

[50] H. Sengar, X. Wang, and A. Nichols, "Call Behavioral analysis to Thwart SPIT attacks on VoIP networks," in *Security and Privacy in Communication Networks*. Springer, 2012, pp. 501–510.

[51] H. J. Kang, Z.-L. Zhang, S. Ranjan, and A. Nucci, "Sip-based voip traffic behavior profiling and its applications," in *Proceedings of the 3rd annual ACM workshop on Mining network data*. ACM, 2007, pp. 39–44.

[52] Y. Bai, X. Su, and B. Bhargava, "Adaptive Voice Spam Control with User Behavior Analysis," in *Proceedings of the IEEE International Conference on High Performance Computing and Communications (HPCC)*, 2009.

[53] R. MacIntosh and D. Vinokurov, "Detection and mitigation of spam in IP telephony networks using signaling protocol analysis," in *Advances in Wired and Wireless Communication, 2005 IEEE/Sarnoff Symposium on*. IEEE, 2005, pp. 49–52.

[54] S. Phithakkitnukoon, R. Dantu, R. Claxton, and N. Eagle, "Behavior-based adaptive call predictor," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 6, no. 3, p. 21, 2011.

[55] H. Yan, K. Sripanidkulchai, H. Zhang, Z.-Y. Shae, and D. Saha, "Incorporating active fingerprinting into spit prevention systems," in *Third annual security workshop (VSWâĂŹ06)*. Citeseer, 2006.

[56] EveryCaller, "Call Control," http://www.everycaller.com.

[57] Budaloop, "Regex Call Blocker," https://play.google.com/store/apps/details?id=com.budaloop.regexblocker.

[58] Pindrop Security, "Fraud Detection System," http://www.pindropsecurity.com/fraud-detection-system.

[59] S. J. Brolin and S. Colodner, "Automatic number identification in subscriber loop carrier systems," Nov. 1 1977, uS Patent 4,056,690.

[60] I. Neustar, "Nanpa : Ani ii digits - view assignments," https://www.nationalnanpa.com/number_resource_info/ani_ii_assignments.html, 2015.

[61] S. Horvath and T. Kasvand, "Voice identification prescreening and redirection system," Sep. 6 2002, uS Patent App. 10/236,810.

[62] D. Reich and R. Szabo, "Method and system of determining unsolicited callers," Apr. 28 2004, uS Patent App. 10/833,515.

[63] C. Pörschmann and H. Knospe, "Analysis of Spectral Parameters of Audio Signals for the Identification of Spam Over IP Telephony." in *CEAS*, 2008.

[64] C. Pörschmann and H. Knospe, "Spectral Analysis of Audio Signals for the Identification of Spam Over IP Telephony," in *Proceedings of the NAG/DAGA International Conference on Acoustics*, 2009.

[65] D. Lentzen, G. Grutzek, H. Knospe, and C. Porschmann, "Content-based Detection and Prevention of Spam over IP Telephony-System Design, Prototype and First Results," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2011.

[66] J. Strobl, B. Mainka, G. Grutzek, and H. Knospe, "An Efficient Search Method for the Content-Based Identification of Telephone-SPAM," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2012.

[67] S. A. Iranmanesh, H. Sengar, and H. Wang, "A Voice Spam Filter to Clean Subscribers' Mailbox," *Security and Privacy in Communication Networks*, 2013.

[68] F. Maggi, "Are the Con Artists Back? A Preliminary Analysis of Modern Phone Frauds," in *Proceedings of the IEEE International Conference on Computer and Information Technology (CIT)*, 2010.

[69] L. R. Rabiner, "Applications of speech recognition in the area of telecommunications," in *Automatic Speech Recognition and Understanding, 1997. Proceedings., 1997 IEEE Workshop on*. IEEE, 1997, pp. 501–510.

[70] David R. Wheeler, "Voice recognition will always be stupid," http://www.cnn.com/2013/08/20/opinion/wheeler-voice-recognition/.

[71] V. A. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. T. Hunter, and P. Traynor, "Pindr0p: Using single-ended audio features to determine call provenance," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 109–120. [Online]. Available: http://doi.acm.org/10.1145/1866307.1866320

[72] H. Hai, Y. Hong-Tao, and F. Xiao-Lei, "A SPIT Detection Method Using Voice Activity Analysis," in *Proceedings of the International Conference on Multimedia Information Networking and Security (MINES)*, 2009.

[73] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, "Detecting SPIT calls by checking human communication patterns," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2007.

[74] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, "Prevention of Spam over IP Telephony (SPIT)," NEC, Tech. Rep., 2006.

[75] J. Lindqvist and M. Komu, "Cure for spam over internet telephony," in *4TH IEEE CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE (CCNC 2007). ProceedingsâĂę vol., n*, 2007, pp. 896–900.

[76] A. Markkola and J. Lindqvist, "Accessible Voice CAPTCHAs for Internet Telephony," in *Proceedings of the Symposium on Accessible Privacy and Security (SOAPS)*, 2008.

[77] Y. Soupionis, G. Tountas, and D. Gritzalis, "Audio CAPTCHA for SIP-based VoIP," in *Proceedings of International Information Security Conference*, 2009.

[78] E. Bursztein and S. Bethard, "Decaptcha: Breaking 75% of eBay Audio CAPTCHAs," in *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2009.

[79] E. Harris, "The Next Step in the Spam Control War: Greylisting," http://projects.puremagic.com/greylisting/whitepaper.html, 2003.

[80] Google Voice, "Screen calls," https://support.google.com/voice/answer/115083.

[81] Verizon, "Call Intercept," https://www.verizon.com/support/residential/phone/homephone/calling+features/call+intercept/130058.htm.

[82] Phone.com, "Phone.com university âĂŞ screening calls for your business line | phone.com," https://www.phone.com/blog/tips-tricks/2014/02/24/phone-com-university-screening-calls-business-line/, February 2014.

[83] N. Croft and M. Olivier, "A Model for Spam Prevention in IP Telephony Networks using Anonymous Verifying Authorities," in *Proceedings of the Annual Information Security South Africa Conference*, 2005.

[84] H. Mustafa, W. Xu, A. R. Sadeghi, and S. Schulz, "You Can Call but You Can't Hide: Detecting Caller ID Spoofing Attacks," in *Proceedings of the Conference on Dependable Systems and Networks (DSN)*, 2014.

[85] K. Ono and H. Schulzrinne, "Have i met you before?: using cross-media relations to reduce spit," in *Proceedings of the 3rd International Conference on Principles, Systems and Applications of IP Telecommunications*. ACM, 2009, p. 3.

[86] A. Back, "Hashcash - A Denial of Service Counter-Measure," http://www.hashcash.org/hashcash.pdf, 2002.

[87] H. Tschofenig, R. Falk, J. Peterson, J. Hodges, D. Sicker, J. Polk, and A. Siemens, "Using saml to protect the session initiation protocol (sip)," *IEEE Network*, vol. 20, no. 5, pp. 14–17, 2006.

[88] S. Saklikar and S. Saha, "Identity federation for voip-based services," in *Proceedings of the 2007 ACM workshop on Digital identity management*. ACM, 2007, pp. 62–71.

[89] L. Kong, V. A. Balasubramaniyan, and M. Ahamad, "A lightweight scheme for securely and reliably locating sip users," in *VoIP Management and Security, 2006. 1st IEEE Workshop on*. IEEE, 2006, pp. 9–17.

[90] V. Balasubramaniyan, M. Ahamad, and H. Park, "Callrank: Combating spit using call duration, social networks and global reputation." in *CEAS*, 2007.

[91] R. Dantu and P. Kolan, "Preventing voice spamming," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), Workshop on VoIP Security Challenges and Solutions*, 2004.

[92] B. Mathieu, Y. Gourhant, and Q. Loudier, "Spit mitigation by a network level anti-spit entity," in *Proc. of the 3rd Annual VoIP Security Workshop*, 2006.

[93] C. Dwork and M. Naor, "Pricing via Processing or Combatting Junk Mail," in *Advances in Cryptology (CRYPTO)*, 1992.

[94] N. Banerjee, S. Saklikar, and S. Saha, "Anti-vamming trust enforcement in peer-to-peer voip networks," in *Proceedings of the 2006 international conference on Wireless communications and mobile computing*. ACM, 2006, pp. 201–206.

[95] C. Jennings, "Computational puzzles for spam reduction in sip," 2007.

[96] S. Niccolini, "Spit prevention: state of the art and research challenges," in *Proceedings of the 3rd Workshop on Securing Voice over IP*, 2006.

[97] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, "On Spam over Internet Telephony (SPIT) Prevention," *IEEE Communications Magazine*, 2008.

[98] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner, "Ise03-2: Spam over internet telephony (spit) prevention framework," in *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE*. IEEE, 2006, pp. 1–6.

[99] D. Gritzalis and Y. Mallios, "A sip-oriented spit management framework," *Computers & Security*, vol. 27, no. 5, pp. 136–153, 2008.

[100] D. Gritzalis, G. Marias, Y. Rebahi, Y. Soupionis, and S. Ehlert, "Spider: A platform for managing sip-based spam over internet telephony spit," *Journal of Computer Security*, vol. 19, no. 5, pp. 835–867, 2011.

[101] R. Dantu and P. Kolan, "Detecting spam in voip networks," in *Proceedings of the steps to reducing unwanted traffic on the internet on steps to reducing unwanted traffic on the internet workshop*. USENIX Association, 2005, pp. 5–5.

[102] M. Hansen, M. Hansen, J. Möller, T. Rohwer, C. Tolkmit, and H. Waack, "Developing a legally compliant reachability management system as a countermeasure against spit," in *Proceedings of Third Annual VoIP Security Workshop, Berlin, Germany*, 2006.

[103] B. Mathieu, S. Niccolini, and D. Sisalem, "SDRS: a voice-over-IP spam detection and reaction system," *Security & Privacy, IEEE*, vol. 6, no. 6, pp. 52–59, 2008.

[104] N. d'Heureuse, J. Seedorf, and S. Niccolini, "A policy framework for personalized and role-based spit prevention," in *Proceedings of the 3rd International Conference on Principles, Systems and Applications of IP Telecommunications*. ACM, 2009, p. 12.

[105] S. Dritsas, V. Dritsou, B. Tsoumas, P. Constantopoulos, and D. Gritzalis, "Ontospit: Spit management through ontologies," *Computer Communications*, vol. 32, no. 1, pp. 203–212, 2009.

[106] M. Scatá and A. L. Corte, "Security analysis and countermeasures assessment against spit attacks on voip systems," in *Internet Security (WorldCIS), 2011 World Congress on*. IEEE, 2011, pp. 177–183.

[107] A. D. Keromytis, "A survey of voice over ip security research," in *Information Systems Security*. Springer, 2009, pp. 1–17.

[108] Keromytis, Angelos D, "A comprehensive survey of voice over ip security research," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 2, pp. 514–537, 2012.

[109] R. Baumann, S. Cavin, and S. Schmid, "Voice over ip-security and spit," *Swiss Army, FU Br*, vol. 41, pp. 1–34, 2006.

[110] S. Phithakkitnukoon, R. Dantu, and E.-A. Baatarjav, "Voip securityâĂŤattacks and solutions," *Information Security Journal: A Global Perspective*, vol. 17, no. 3, pp. 114–123, 2008.

[111] V. M. Quinten, R. Van De Meent, and A. Pras, "Analysis of techniques for protection against spam over internet telephony," in *Dependable and Adaptable Networks and Services*. Springer, 2007, pp. 70–77.

[112] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, "Issues and challenges in securing voip," *computers & security*, vol. 28, no. 8, pp. 743–753, 2009.

[113] S. Dritsas, Y. Soupionis, M. Theoharidou, Y. Mallios, and D. Gritzalis, "Spit identification criteria implementation: Effectiveness and lessons learned," in *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*. Springer, 2008, pp. 381–395.

[114] G. F. Marias, S. Dritsas, M. Theoharidou, J. Mallios, and D. Gritzalis, "SIP vulnerabilities and anti-SPIT mechanisms assessment," in *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*. IEEE, 2007, pp. 597–604, http://dx.doi.org/10.1109/ICCCN.2007.4317883.

[115] S. F. Khan, M. Portmann, and N. W. Bergmann, "A Review of Methods for Preventing Spam in IP Telephony," *Modern Applied Science*, vol. 7, no. 7, p. p48, 2013.

[116] J. Rosenberg, C. Jennings, and J. Peterson, "The session initiation protocol (SIP) and spam," RFC 5039, January, Tech. Rep., 2008.

[117] M. W. Slawson and C. I. O. C. Waiting, "Caller ID Basics," *Intertek Testing Services/Testmark Laboratories, Lexington, KY*, 2001.

APPENDIX

Description	Decimal	ASCII	Hex
Message Type (MDMF)	128		80
Message Length	33		21
Parameter Code (Date & Time)	1		01
Parameter Length	8		08
Month (November)	49	1	31
	49	1	31
Day (28)	50	2	32
	56	8	38
Hour (3pm)	49	1	31
	53	5	35
Minutes (43)	52	4	34
	51	3	33
Parameter Code (CPN)	2		02
Parameter Length (10)	10		0A
From (6062241359)	54	6	36
	48	0	30
	54	6	36
	50	2	32
	50	2	32
	52	4	34
	49	1	31
	51	3	33
	53	5	35
	57	9	39
Parameter Code (Name)	7		07
Parameter Length (9)	9		09
Name (Joe Smith)	74	J	4A
	111	o	6F
	101	e	65
	32		20
	83	S	53
	109	m	6D
	105	i	69
	116	t	74
	104	h	68
Checksum	88		58

Table III: MDMF message sample in the existing POTS protocol [117].