Phoneypot: Data-driven Understanding of Telephony Threats

Payas Gupta
New York University
Abu Dhabi
payasgupta@nyu.edu

Bharat Srinivasan
Georgia Institute of Technology
bharat.srini@gatech.edu

Vijay Balasubramaniyan
Pindrop Security
vijay@pindropsecurity.com

Mustaque Ahamad
Georgia Institute of Technology
New York University Abu Dhabi
mustaq@cc.gatech.edu

Abstract—**Cyber criminals are increasingly using robocalling, voice phishing and caller ID spoofing to craft attacks that are being used to scam unsuspecting users who have traditionally trusted the telephone. It is necessary to better understand telephony threats to effectively combat them. Although there exist crowd sourced complaint datasets about telephony abuse, such complaints are often filed after a user receives multiple calls over a period of time, and sometimes they lack important information. We believe honeypot technologies can be used to augment telephony abuse intelligence and improve its quality. However, a telephony honeypot presents several new challenges that do not arise in other traditional honeypot settings. We present Phoneypot, a first large scale telephony honeypot, that allowed us to explore ways to address these challenges. By presenting a concrete implementation of Phoneypot using a cloud infrastructure and 39,696 phone numbers (phoneytokens), we provide evidence of the benefits of telephony honeypots. Phoneypot received 1.3 million calls from 250K unique sources over a period of seven weeks. We detected several debt collectors and telemarketers calling patterns and an instance of a telephony denial-of-service attack. This provides us with new insights into telephony abuse and attack patterns.**

I. Introduction

> "Hello, this is Rachel at cardholder services[1], calling in reference to your current credit card account. . . . Please press the number 1 on your phone . . . Or press the number 2 . . ."

In the United States, many have received such call, or one like it. Perhaps similar calls come to unsuspecting people in other countries. The frequency of such unwanted calls (also called telephony spam) on our phones has increased at an alarming rate. The Federal Trade Commission (FTC) has received millions of complaints from citizens about such unwanted and fraudulent calls. Recent increase in attacks over the telephony channel can be attributed to the availability of IP telephony (Voice over Internet Protocol). Such calls can be made at no or low cost at scale in an automated fashion similar to email spam, and criminals are already exploiting the telephony channel to craft attacks such as voice phishing (vishing). Unfortunately, attacks that utilize the telephone as a resource are more successful because people in the past have trusted the telephony channel. In fact, telephony has reportedly become the weak link even for web security because cyber criminals have used social engineering over the phone to reset online banking credentials to steal money [48].

News articles have repeatedly highlighted recurring scams relying on telephony such as the tech support scam [17], Nigerian scam [1], credit card scam [12] and the one-ring/missed-call scam [26], [16], also known as Wangiri fraud [25]. In the past, phone numbers have been proven to be quite effective in nailing down illicit actors. Consumer protection agencies such as the FTC have already taken down some scam operations in this space [9], [8], [10], [7], and researchers have tried to understand the phenomenon using empirical analysis [42], [43], [44], [51]. Researchers have also used crowd sourced datasets like 800notes [5] to understand how telephony scams evolve e.g. Nigerian scam [41]. However, there exist many limitations of the self-reported datasets like FTC's fraudulent complaint database and 800notes.

To gain a better understanding of telephony abuse, we manually examined complaints both from the FTC and 800notes crowd sourced complaint datasets and analyzed them on completeness, accuracy and timeliness. Since 800notes includes detailed comments about an abuse instance, we use it to illustrate how the quality of telephony abuse intelligence needs to be improved.

1) **Completeness:** It is desirable to have as much intelligence as possible to have a complete picture of a certain threat. It can be argued that when reports come from a large set of users, the complaint set should be reasonably complete. However, we have no way to demonstrate this without a systematic exploration of telephony scams.
2) **Accuracy:** A telephony abuse report should describe who made the call, the time at which the call was made, and information about the call that provides evidence of it being abusive. Accuracy of such a report means that the source and time are recorded correctly and its description is objective and supports why it is abusive. We found that due to the open

[1] The Federal Trade Commission (FTC) sponsored the Zapping Rachel contest at 2014 DefCon on using honeypots to combat robocallers. More information about Zapping Rachel is at http://www.ftc.gov/zapping-rachel.

NDSS '15, 8-11 February 2015, San Diego, CA, USA
Copyright 2015 Internet Society, ISBN 1-891562-38-X
http://dx.doi.org/10.14722/ndss.2015.23176

nature of 800notes forum, complaints on it are not limited to telephony fraud; people use this platform to complain about almost anything, like email spam, SMS spam, voice spam etc. This results in noisy data where all complaints do not pertain to telephony abuse. It is possible that different people perceive calls from a source differently and may disagree with others about the reported number belonging to a fraudulent caller. We found reports on 800notes with completely opposite opinions about a spam call source. In particular, we found conflicting opinions about the call source actually being a major bank. It could also be possible that the illicit actors themselves are reporting positive reviews about calls from phone numbers that are used by them. The noisy and conflicting nature of user reports impacts the accuracy of such datasets. Also, we found complaints without the actual time of a fraud call and are also unclear about the number of calls received.

3) **Timeliness:** Timeliness refers to how soon a report is filed after an abuse call is received. We found that there is a delay between when the fraudulent calls are made to people and when they are reported by them to FTC or 800notes. Generally, abuse calls and the phone numbers from where they come are reported after several days or sometimes even weeks after the time when the first call was received. Also, people report a source only when they have been called multiple times, which also contributes to a delay.

Although methods for collecting data in the crowd sourced datasets can be improved [49], we believe accuracy, timeliness and completeness are inherent challenges that will be faced by such datasets. This is because users are often interrupted by abuse calls when they may be busy with important activities and expecting them to report all such calls accurately in a timely manner would be impractical. Therefore, in this paper we propose Phoneypot, a first large-scale telephony honeypot, to explore the feasibility of augmenting abuse information available in existing crowd sourced and self-reported datasets like 800notes and FTC complaint database. A telephony honeypot should be capable of receiving, recording and monitoring calls coming to it. Thus, by setting up a telephony honeypot, we entice the attackers to make calls to phone numbers associated with it. We define the term phoneytokens that are phone numbers associated with a set of features e.g. age, geography and history. Phoneytokens are a key requirement and form the building blocks for a telephony honeypot.

Unlike traditional honeypots that are used to study online threats, telephony honeypots present several new challenges. Phone numbers and hence phoneytokens are a limited and regulated resource that is not true for other resources like email addresses. Also, phone numbers have attributes like geography and age, which need to be considered. Telephony honeypot implementation must also consider various ways in which calls destined to phoneytokens could be received and how callers can be engaged to obtain information about the purpose of the call. Misdialed calls to phoneytokens cannot be ruled out because a phoneytoken may be similar to a legitimate phone number. These challenges must be addressed before a telephony honeypot could become a valuable source of threat intelligence.

In this paper, we argue the need for a telephony honeypot, possible ways to build it, and demonstrate its use to augment the intelligence available from other telephony abuse datasets that currently exist. Our major contributions in this paper can be summarized as follows.

1) There has been numerous reports about the scope and magnitude of telephony spam and scams, however, to the best of our knowledge, we are the first to systematically study them by using a large-scale telephony honeypot. We show how such a honeypot presents several new challenges compared to traditional honeypots and we explore ways in which these challenges can be addressed.
2) We report results from the deployment of a first large-scale telephony honeypot. We worked with an industry partner to build Phoneypot, which is a concrete instance of such a telephony honeypot. Phoneypot uses phone numbers obtained from a cloud communication service provider with 39,696 phoneytokens. Once Phoneypot was deployed, over a period of seven weeks, we received close to 1.3 million unsolicited calls to phone numbers associated with these phoneytokens. These calls came from a total of 252,621 unique sources, including sources that made a large number of calls.
3) Our analysis of the calls that Phoneypot received revealed several abuse or attack patterns. For example, we detected several debt collector and telemarketers calling patterns and an instance of a telephony denial-of-service attack. We also observed the significance of the number block issue date (i.e. age) of a phoneytoken. Using t-test, we found that the difference between the total number of calls received on phone numbers that came from older blocks as compared to phone numbers from newer blocks is highly significant.
4) We compared the timestamps of reports associated with fraudulent phone numbers on the FTC fraud complaint database, to the time when Phoneypot received a call from the same number. We found strong evidence that Phoneypot can be used to complement the current datasets and can help mitigate the timeliness problem. Phoneypot also received calls that were not reported on the other data sources and hence could also improve completeness.

We believe a telephony honeypot can help us better understand telephony abuse and attacks. It is the goal of this paper to put this hypothesis on an empirical footing.

II. Background and Related Work

In this section we present work related to telephony abuse (see Section II-A) and honeypots (see Section II-B).

A. *Phishing, Vishing & SPIT*

Phone spam in its very basic form has shown similarities to email spam [20]. Low operating costs, high return on investment, scalability, reachability and anonymity are some of the shared attributes between the two channels that are leveraged by scamsters [11]. Thus, it is worth reflecting on existing solutions that are in place to counter email spam. Pitsillidis *et al.* [55] discuss the rich and diverse set of spam data feeds that has served as intelligence inputs in the email space. They range from botnet datasets, MX honeypots, seeded honey accounts, human identified spam email-messages and domain blacklists. If we compare this to sources like the FTC phone fraud complaint database [19] that is currently available, there is a huge gap that needs to be filled.

For instance Jiang *et al.* [42], [43] rely on customer generated reports [5] to identify instances of international revenue sharing fraud [15] in call detail records corpora. Also, calls and messages to/from premium rate numbers [42] and services must be leveraged to create blacklists for potentially vulnerable telephony endpoints. A telephony honeypot can serve this purpose by logging activity associated with suspicious phone numbers, their associated voice fingerprints [35], the transcribed message templates, calling/messaging patterns (timing, frequency etc.) [33], [34], [68] and other metadata.

B. *Honeypots*

Honeypots have tremendous potential for the security community – in principle it is an information system resource whose value lies in an unauthorized or illicit use of that resource [65]. Honeypots have been proposed and used effectively in various domains. In traditional networks they have complemented intrusion detection systems [54], [62] and firewall mechanisms well. They have been used to fight email spam [61], to characterize worms, botnets, malware and DDOS attacks [66], [37], [55], [57], to deceive network fingerprinting tools [57], [58] and counter web server abuse [45]. They have been proposed in the context of detecting database access breaches [13], in detecting SMS spammers in cellular networks [43], for specific deployment in wireless networks [27], and in general to protect large enterprises [47]. They have also been proposed in the Voice over IP domain [67], [53], [38], [24], [36] to combat voice spam or spam over internet telephony (SPIT) [39], [68], [33], [34], [50], [60], [63], [64], and to prevent vishing [49], [40], [23], [59], [46]. Telephony honeypot seeks to serve a similar purpose in the telephony domain with some key differences from works aforementioned. It monitors spam calls irrespective of origination or path traversed, be it PSTN, cellular or VoIP. This is useful if one takes into account the architecture of current telecommunication networks where we have a mix of cellular, VoIP and traditional PSTN networks interacting with each other and calls being routed across them.

Although, conceptually the idea of a honeypot is similar across domains, the decisions pertaining to their design and deployment have varied. Provos *et al.* [58] elaborate on how a passive v/s a highly interactive honeypot may affect its design. Similarly, a decision on having a physical honeypot as opposed to a virtual honeypot [57], [56] would most likely affect the scale and flexibility of its deployment. Telephony honeypot deviates from the strict definitions above and takes a hybrid approach. It can make use of a cloud infrastructure to set up phoneytokens and other elements of the telephony stack. Thus, the infrastructure can be virtualized while the phone numbers remain real.

Techniques used to setup honeypots have also varied. Email spam traps have been setup by configuring the MX record for a domain to point to an SMTP server that accepts all inbound messages but has no legitimate email addresses [61]. They have also been setup by having seeded honey accounts created across a range of e-mail providers whose sole purpose is to capture unsolicited e-mail [55]. Jiang *et al.* [43] used grey phone numbers (which are phone numbers associated with devices that are not supposed to communicate with other mobile numbers using SMS) to set up SMS spam traps at the cellular network level.

III. Telephony Honeypot Challenges

As mentioned in section I, telephony honeypots have important differences compared to traditional honeypots that are deployed to collect Internet threat information. As a result, there are several new challenges that must be addressed before setting up the telephony honeypot. We outline these challenges and discuss how Phoneypot, our implementation of a telephony honeypot deals with them in the next section.

A. *Cost*

Some of the resources used in traditional honeypots can be easily acquired (e.g., email addresses) at no or low cost. In contrast, phone numbers are a limited and managed resource; obtaining a sizable and diverse pool of phoneytokens and routing calls to them may incur significant costs. This is because transport of the calls may require SIP trunking and a telecommunications carrier may charge based on call duration and frequency. In some regions of the world, both the calling and called parties are charged by the carriers irrespective of the direction of the call. However, in countries like India only outgoing calls are charged and incoming calls are free. Although actual costs depend on possible deployment options discussed in the next section, there could be both initial and recurring costs that could be significantly higher than the cost of operating a traditional honeypot infrastructure.

B. *Ability to engage callers*

Telephony is a synchronous interaction channel where the caller's actions often depend on the called party picking up and responding to the call. Engaging the caller to fully learn the purpose of the call is a major challenge in setting up a telephony honeypot. We suspect that engaging a caller actively as compared to passively via voicemail would be more effective. Actively engaging calls would incentivize the caller to stay longer on the call and thus give us an audio file of desired size that can be examined for caller intent. Several levels of interactions are possible in a telephony honeypot.

1) **No interaction:** When a call is received at a telephony honeypot, it can choose to either provide a busy signal (SIP response 486) or decline (SIP response 603) the call immediately. This avoids call completion charges and could provide useful information. For example, the honeypot can record calling and called phone numbers and a timestamp that captures when the call was made, and if possible network level SIP signaling metadata.
2) **Low interaction:** Low level of interaction can be achieved by setting up a voicemail. This may result in no voicemail being left by the scamsters, as they

might not be interested in leaving any message. However, in the case of a robocall, we may end up recording the audio at the least.

3) **Medium interaction:** We can provide automated medium level of interaction by setting up an IVR, which is in form of a conversation. More creative the message the better it is. For example, the voice message can include sentences like "I am not able to hear you, can you please repeat . . ., Yes I can listen to you now, please go ahead . . .".
4) **High interaction:** High level of meaningful interaction in an automated fashion is challenging. One can set it up using an automated conversation engine that performs speech recognition from the audio of the incoming calls and automatically engages callers in multiple rounds of communication. Once sources that originate high number of calls are identified, a limited number of calls from them can be handled manually to provide a high level of interaction. This can help gain more complete information about the purpose of the calls.

C. Legal: Telephone call recording laws

Recording of telephone calls is strictly regulated in many countries. For example in the United States, there are some states (e.g. California) which require all party consent before a call can be recorded but others (e.g. Georgia) only require single party consent [18]. The California Supreme Court has ruled that if a caller in a one-party state records a conversation with someone in California, that one-party state caller is subject to the stricter of the laws and must have consent from all callees. Thus, a telephony honeypot must address consent requirements if it chooses to record calls.

D. Seeding of phoneytokens

Ideally, a telephony honeypot would like to receive calls from fraudsters and no calls from legitimate users. For such calls to come, the caller must know the phone numbers that belong to the honeypot. Seeding of phoneytokens refers to the process by which phoneytokens are publicized so they can be discovered by attackers. For example, similar to email addresses, attackers can use crawlers to discover phone numbers and people or organizations associated with them. There exist phone number lists like "Do Not Call List" where phoneytokens can be posted. In general, seeding of phoneytokens requires that they be posted on a variety of targets of fraudsters, including social media and websites. For example, one can create accounts with various profile characteristics that include phone numbers. The primary challenge with phoneytokens lies in the automation of seeding them. Posting phoneytokens only from fake accounts at a high rate may either be flagged as spam or might result in blocking the account altogether. Therefore, the posts should adhere to the policies of the site so that the account that publishes phoneytokens is not blocked. Moreover, potential target websites have different structures and layouts; therefore it is challenging to automate phoneytoken posting which is essential for a large-scale honeypot deployment.

E. Evading detection of the telephony honeypot

The telephony honeypot should mimic a normal end point user, which depends on the level of engagement mentioned previously. For example a normal hang up (SIP response 486) as opposed to decline (SIP response 603). Telephony honeypot should be configured to use proxy for RTP traffic; otherwise IP address of the honeypot might be leaked.

F. Avoiding false positives

Because of the limited space of phone numbers and how people dial numbers, it is possible to misdial a phone number. Also, to make a phoneytoken attractive to attackers, it could be seeded where legitimate people may find and dial it. A misdialed call to a phoneytoken leads to a false positive. Although it is difficult to avoid misdialing completely, several precautions can be taken. Phoneytokens can be seeded in such a way that legitimate people are less likely to call phone numbers associated with them. For example, while advertising or posting on discussion forums, the posts should be enticing but at the same time they should not appeal to legitimate users.

IV. Telephony Honeypot Implementation Options

A telephony honeypot is nothing but a communications server that has the capability to receive, make and record calls. As mentioned earlier, the phone numbers on which a telephony honeypot receives calls are called phoneytokens. A phoneytoken is a digital resource i.e., a phone number with associated features like age, geography or historical profile, whose value lies in an unauthorized use of that resource. Phoneytokens are unique and are not assigned to any entity; therefore, no legitimate person should be using or accessing them. However, there could be false positives. For example, a confused user can mistakenly use a phoneytoken by dialing a wrong number.

The allocation and assignment of phone numbers is coordinated and typically one must work with a telecommunication carrier to acquire phoneytokens. Ideally, the set of phoneytokens acquired for a honeypot would have diverse profiles as mentioned earlier. Phoneytokens typically have a cost associated with them that can impact the size of their pool available for a telephony honeypot.

An instance of a telephony honeypot can be built on top of any telephone PBX such as open source framework like Asterisk [2] for building communications applications or using cloud communication service providers. At the minimum, a telephony honeypot should have the capability to log the source phone number, the destination phone number and the timestamp of the call. In the following section, we provide other functionalities a telephony honeypot can be equipped with.

A. Telephony honeypot functionalities

1) **Voicemail/IVR:** Unlike email, phone calls are synchronous in nature and require interaction from the target endpoint. Voicemail and Interactive Voice Response (IVR) are necessary to build an interaction based telephony honeypot. One can leverage this to setup different interaction levels with the caller in an automated way.
2) **Call recording feature:** Since signatures can be computed using audio analysis [35], the telephony honeypot should ideally have support for recording

calls. This will also help us to transcribe the audio and perform voice analysis to differentiate between a robocaller and a human caller. The call audio can provide additional information about nature and purpose of a call.

3) **Availability of full CDRs:** Call detail records or CDRs capture considerable amount of metadata about incoming and outgoing calls, including source and target phone numbers, time and duration, phone number to which call should be billed, telecommunication equipment information etc. Usually most of the communication servers and service providers can provide full CDRs to the client.

4) **Network logs:** Network logs can provide a lot of information which might not be available in CDRs. Additional information includes gateway IP addresses in case of VoIP calls, routing information, packet size, network latency between calls, codecs used etc.

B. *Setup using communication server*

Having discussed some of the functionalities of a telephony honeypot in the last section, in this section we describe how to build a telephony honeypot on top of Asterisk [2] (similar setup can be used with FreeSwitch [6]).

Asterisk (a free and open source software) turns an ordinary computer into a communications server. Asterisk powers IP PBX systems, VoIP gateways, conference servers and more. Asterisk is capable of interfacing with many traditional telecom protocols, VoIP protocols, and codecs. It provides a comprehensive list of capabilities and features including IVR voicemail, call recording, full CDRs etc.

Following are some of the plausible directions one can follow to setup a telephony honeypot. It can either be integrated with an existing network or set up from scratch.

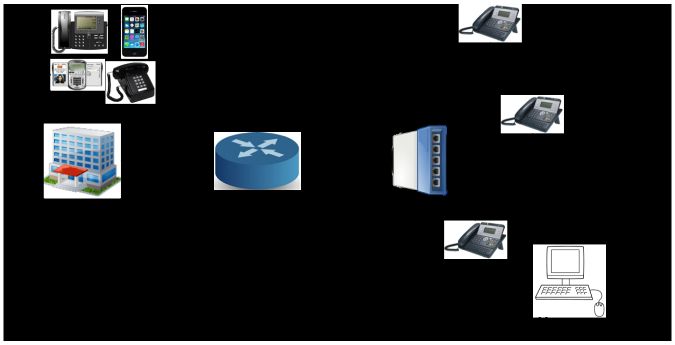


Fig. 1. Telephony honeypot setup for landline numbers using SIP trunk

a) SIP Trunk: SIP trunking is a VoIP and streaming media service based on the Session Initiation Protocol (SIP) by which ISPs deliver telephone services to customers equipped with SIP-based Private Branch Exchange IP-PBX. IP phones, fax machines can all use the PBX to connect with the SIP trunk (see Figure 1). The PBX is responsible for routing calls to the appropriate extensions based on the entry in the call manager table. For example, in Figure 1, an incoming call to 83345 is forwarded to the IP phone with IP address 192.168.1.11. Similarly, any call to a range of numbers (88800-88899) is forwarded to the honeypot with IP address 192.168.1.10. This setup is expensive due to high cost of SIP trunks and would require significant investment in terms of infrastructure and money. For example, to be able to handle concurrent calls, the organization will have to be equipped with E1 or T1 phone lines that allow calls to be multiplexed [3]. A T1 line will allow up to 24 concurrent calls but has a very high cost (≈1000-1500 USD per month). Moreover, a card for connecting the lines to the communication server that runs the Asterisk PBX costs over 3000 USD for handling up to 240 channels. One weakness of this configuration is that it can only handle calls to landline/IP phones unless a GSM gateway is attached (see VoIP GSM gateway below).

b) Integration with the existing IT infrastructure: This setup is similar to the previous one (see Figure 1), however, rather than buying everything and building the whole network from scratch, one can integrate the honeypot with the existing IT network of any institution/company. This can be done by allocating a set of numbers which are not assigned to anyone in the respective institution/company and configuring the PBX to forward any calls coming in to those numbers to the honeypot. This is a low cost option but it limits the diversity of phoneytokens that can be used with the honeypot because all phone numbers come from the pool that is allocated to the organization. Also, this solution is only possible if the IT infrastructure is based on VoIP.

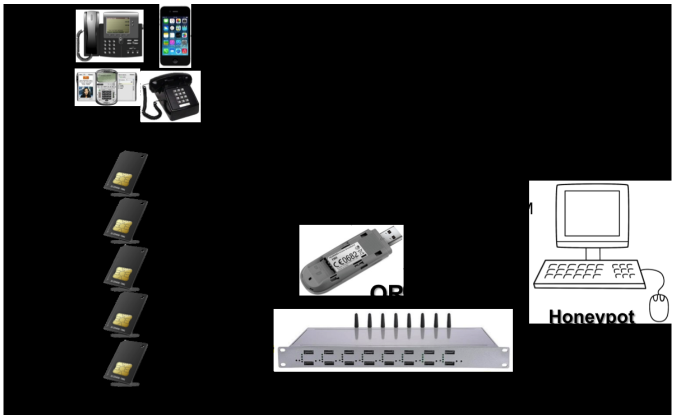


Fig. 2. Telephony honeypot setup for mobile phone numbers using VoIP GSM gateways/USB Wifi Dongle

c) VoIP GSM Gateway: GSM gateways work by inserting a normal Mobile SIM Card into the device, and once signal has been found the device is capable of routing numbers out via the SIM Card. GSM gateways are available in various configurations based on 1, 2, 4 or up-to 128 slots i.e. up-to 128 SIM cards can be added to the GSM gateway. GSM gateways are usually very expensive. A 4-slot GSM gateway can cost up-to 500 USD. Therefore, to scale this setup one can either buy more GSM gateways or purchase more SIM cards and use the unconditional call forwarding feature (which every telecom company provides) to forward all the calls to any of the SIM cards installed in the GSM gateway. In countries like China and India, where the penetration of mobile phones has tremendously increased in the last decade, installing GSM gateways has an advantage to SIP trunks where the influx of unwanted calls is higher on the mobile lines than landlines [4].

d) USB Modem/Dongle with SIM card: These devices/dongles are commonly used to get wireless Internet connection on the laptop while on the move. These dongles (e.g. Huawei E220 [14]) have an in-built GSM chip which interacts with the GSM SIM present inside. Usually the SIM is data only, however, voice enabled SIM cards can be inserted into unlocked versions of the device. The device can directly be connected to a telephony honeypot and can be configured to receive calls. Scalability is a major issue with such a configuration, however, as discussed above, more SIM cards can be purchased and all the calls coming in to these SIM cards can be forwarded to the device. These devices are relatively inexpensive and cost less than 30 USD.

C. *Setup using cloud communication service providers*

There are cloud communication companies (e.g. Tropo [21] and Twilio [22]), which provide telecommunication Infrastructure as a Service (IaaS) to programmatically make and receive calls. For our purpose, one can opt for different services like buying phone numbers (phoneytokens), call recording, transcription etc. The cost is recurring and is based on usage. Call handling and recording is done at the service provider's end. The main advantage of using this kind of setup is that one can choose phone numbers from different locations across the world. For example, with Tropo, one can purchase numbers from more than 40 countries.

V. Phoneypot Deployment

In this section, we provide the details of Phoneypot, a concrete instance of a telephony honeypot, that we used to explore the feasibility and value of telephony honeypots. To the best of our knowledge, Phoneypot is the first and the largest telephony honeypot ever deployed that can receive calls originating from all kinds of sources. We briefly describe how we addressed the challenges associated with telephony honeypots in setting up Phoneypot.

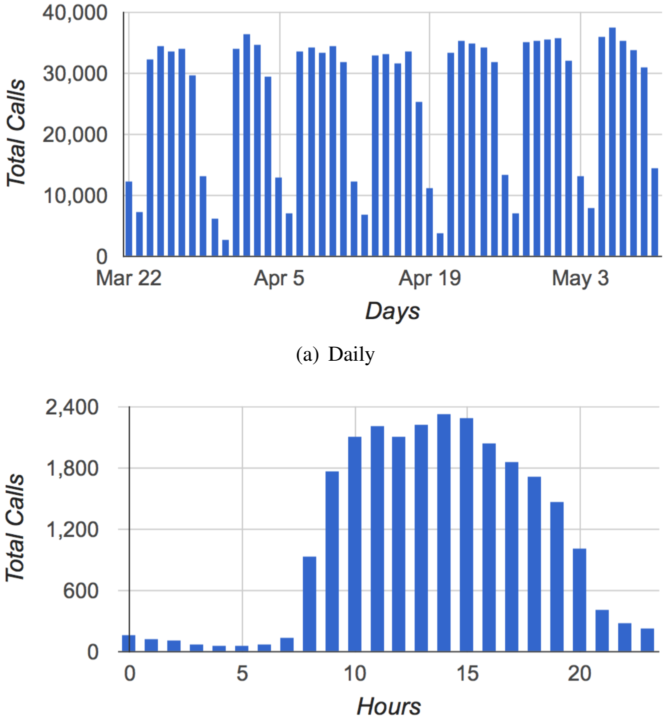
We worked with an industry partner, Nomorobo, to setup Phoneypot with 39,696 phoneytokens obtained from a cloud based telecommunications service provider, where Nomorobo bears the cost of the setup. Nomorobo blocks unwanted robocalls targeting its customers and was keen to use intelligence provided by Phoneypot to enhance the effectiveness of its solution. As discussed earlier, phoneytokens can be seeded at targets that are most likely to be scraped by the scamsters. At this point, we do not actively seed any of the phoneytokens by ourselves. However, according to the provider of these phoneytokens, they are "dirty" based on past history i.e. they have been given up by its customers because of the high volume of unwanted incoming calls as compared to other numbers. We have not been provided any information about the past history of the number of calls on these phoneytokens when they were given up. We also did not record any audio from the calls received on these phoneytokens for now, avoiding cost and legal issues. All the calls coming in to Phoneypot were immediately terminated by sending a busy tone. The only data obtained was the source phone number, the destination phone number and the timestamp of the call. Nomorobo shared this data with us on a weekly basis. In our ongoing work, we are exploring the feasibility of engaging a limited number of "suspicious" callers and recording of call audio.

VI. Results

The main purpose of the early experimental results discussed in this section is to demonstrate the viability of the telephony honeypot idea and to gain early insights. These results are based on deployment of Phoneypot over seven weeks, from 22nd March 2014 till 11th May 2014. We present call volume and temporal analysis of the received calls. We also analyze the effect of age and geography of phoneytokens on call volume. The information recorded by Phoneypot allowed us to identify certain abuse patterns that are discussed in this section.

A. *Call volume and Temporal characteristics*

We received a total of 1,297,517 calls over the course of 50 days that were made to 36,912 phoneytokens. There are a total of 252,621 unique sources that called Phoneypot. It should be noted that despite the claim from the service provider that these numbers are all dirty, we did not receive any calls on 2,784 phoneytokens during this period.



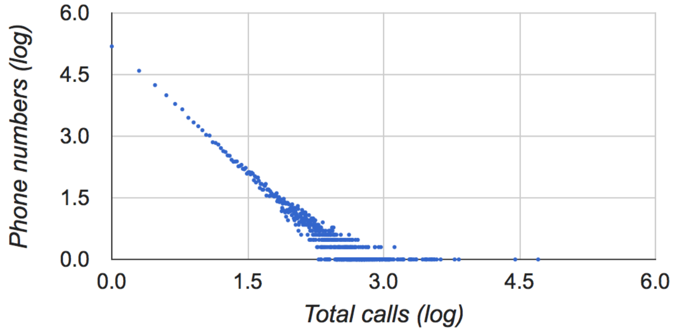
(a) Daily

(b) Hourly

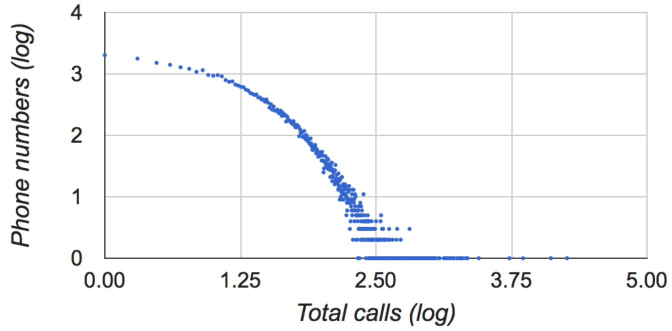
Fig. 3. Diurnal Call Volume

Figure 3(a) shows the call volume on a daily basis. On an average, Phoneypot received approximately 26K calls per day. This is high considering the fact that these phone numbers are not assigned to anyone and are indeed Phoneypot numbers (phoneytokens). As we can also notice, weekday call volume (≈33K) is much higher than weekend call volume (≈8K). Moreover, we can observe from Figure 3(b) that majority of the calls are being made during business hours. More calls on weekdays and during business hours demonstrate that most of the sources want to blend in with the normal telephony traffic to appear legitimate. It should be noted that the time zone used was specific to the time zone of the phoneytoken. For example, if the phone number's area code is from New York then the time zone used was UTC-4, and if it is from California then UTC-7. We lack some data for 31st March because of instability in our collection infrastructure.

B. Call distribution



(a) Outgoing call distribution for sources



(b) Incoming call distribution for phoneytokens

Fig. 4. Log-Log distributions of calls from sources and calls to phoneytokens

In Figure 4(a) and 4(b), we show the outgoing call (calls from sources) and incoming call (calls to phoneytokens) distributions to Phoneypot respectively on a log-log scale. As we can observe, both are heavily tailed, indicating that there are certain sources/destinations which are making/receiving significantly higher number of calls than others. This is very similar to power law distribution seen on the web [32].

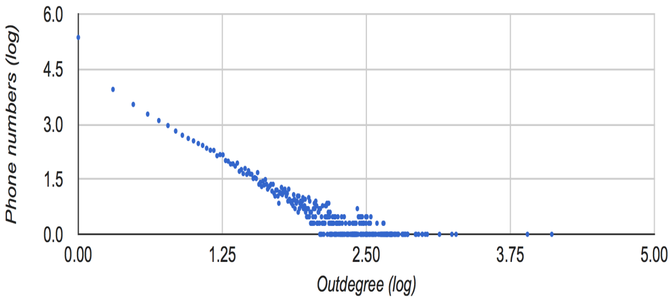


Fig. 5. Log-log outdegree distribution of all sources of Phoneypot

In Figure 5, we show the outdegree distribution on a log-log scale. Outdegree of a source is defined as the total number of phoneytokens to which calls were made from that source. As it can be seen, this graph is heavily tailed as well, which indicates that there are many sources that are reaching out to many phoneytokens. There are even sources that are making calls to ≈10K phoneytokens. Both Figure 4(a) and 5, indicate that there are sources that try to maximize their efforts by making large number of calls to many phone numbers. This is a typical pattern for telemarketers. On the other hand, there exists sources that are making lot of calls to very few phone numbers. We observed that this typical pattern for debt collectors. Please refer to Section VIII-B for more details. Alternatively in the case of Telephony Denial of Service attacks, there are many sources making huge number of calls to one destination in a short period of time (see SectionVIII-A).

C. Age based characteristics

Phone numbers conform to a numbering plan and are allocated to service providers in blocks in a coordinated fashion (service providers make them available to their customers). The North American Numbering Plan (NANP) is an integrated telephone numbering plan that encompasses 25 countries and territories primarily in North America, the Caribbean, and U.S. territories. Thus, some blocks of numbers may be in use for a long time while others could be very recent. Phone numbers with old NPA-NXX introduction versions are more likely to receive spam calls than other numbers. This is because these numbers have already been publicized over the years at different locations and would have been propagated widely.

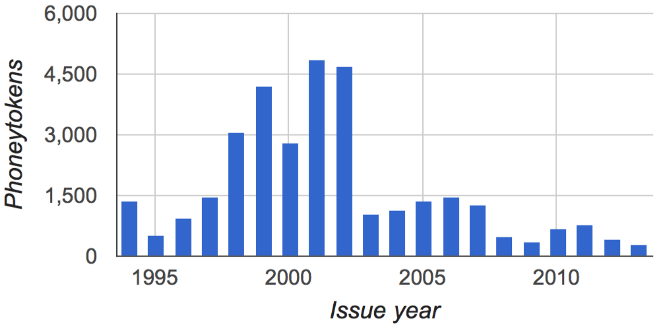


Fig. 6. Age distribution of phoneytokens

We were able to find the issue date of the NPANXX block for only 33,271 phoneytokens. 24,985 phoneytokens were from older blocks (year $<$ 2004) whereas 8,286 (year $\geq$ 2004) were from newer blocks [30]. Figure 6 shows the age distribution of the phoneytokens in Phoneypot.

Since the number of phoneytokens from older blocks is greater than the newer blocks, we normalized the number of incoming calls per phoneytoken. As shown in Figure 7, we can observe that the phoneytokens with older NPA-NXX received more calls as compared to the ones from the newer phone number block range. This may be attributed to the fact that more of these numbers have existed in fraudster databases before they have been ported to Phoneypot than the newer ones, and hence are more likely to receive spam calls. To verify our conjecture, we used a t-test assuming unequal variance. In t-test, the p-value determines the significance level of the difference between two groups. A lower p-value (anything less than 0.05) would imply a significant difference between the

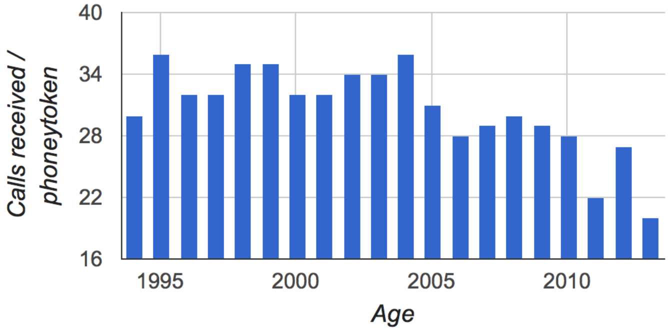


Fig. 7. Age based distribution of the incoming calls per phoneytoken to Phoneypot

groups, something we can use to derive conclusions. We used a two-tailed test, as there was no conclusive evidence to support the use of a one-tailed test.

TABLE I. T-TEST ON TOTAL CALLS RECEIVED BY PHONEYTOKENS BASED ON ITS AGE

Groups	N	μ	σ	P(T≤t)
< 2004	10	33.2	1.87	0.005
≥ 2004	10	28	4.4	

The p-value of 0.005 (see Table I) shows that there is a significant difference between the two groups which is sufficient to conclude that the phoneytokens from the older blocks will receive higher number of calls.

D. Geographical characteristics

Population characteristics vary with geography even in one country; for example, Florida has the densest concentration of older people in the USA. It is believed criminals and scamsters have targeted older people in the pastand the same could be true for vishing attacks. By having phoneytokens that come from number ranges allocated to various geographical locations, we can hope to better understand such questions.

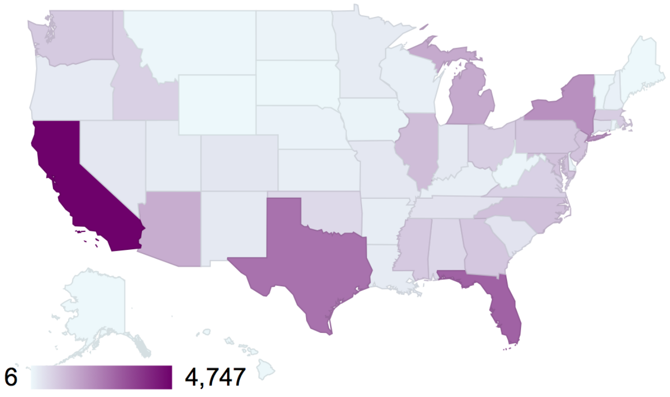


Fig. 8. Geographical distribution of the USA phoneytokens based on area code

Out of 39,696 phoneytokens, majority (33,267) were from the USA and rest (190) from Canada. We also had 6,239 toll free numbers in the pool of phoneytokens. Toll free numbers are numbers that begin with one of the following three-digit codes: 800, 888, 877, 866, 855 or 844. Figure 8 shows choropleth chart of the USA phoneytokens based on geography. It provides an easy way to visualize how the phoneytokens were distributed across the USA aggregated over states. Geographical distribution is determined solely based on the NPA or the area codes.

We obtain the population data from US Census [29]. To investigate this, we divided the states in two groups based on various factors.

e) Total population per phoneytoken: The null hypothesis states that there are no differences between the calls coming to the states with higher population (>4M), compared to those with the states with lesser population (≤ 4M). While there are differences, the p-value of 0.153 is not significant enough to conclude that the population per phoneytoken makes any difference (refer Table II).

TABLE II. T-TEST ON TOTAL CALLS RECEIVED BASED ON TOTAL POPULATION PER STATE

Groups	N	μ	σ	P(T≤t)
> 4M	26	31.23	6.10	0.153
≤ 4M	25	28.28	8.20	

f) Elderly population per phoneytoken: The null hypothesis states that there are no differences between the calls coming to the top 5 states with higher population (>15%) of elderly people, compared to states with lesser population (≤ 15%) of elderly people. The results are shown in Table III. While there are differences, the p value of 0.621 is not significant enough to conclude that the population with different age groups makes any difference which is contrary to the popular belief that states with elderly people receive more calls.

TABLE III. T-TEST ON TOTAL CALLS RECEIVED BASED ON ELDERLY POPULATION PER STATE

Groups	N	μ	σ	P(T≤t)
> 15%	5	13.2	5.35	0.311
≤ 15%	46	14.13	3.86	

g) Immigrant population per phoneytoken: Based on a reported study of the recent IRS telephony scam [31], it is believed that phone fraudsters are targeting immigrant population. The null hypothesis states that there are no differences between the calls coming to the states with higher percentage (> 2.2%) of population of Asian immigrants, compared to those with states with lesser percentage (≤ 2.2%) of Asian immigrant population. The results are shown in Table IV. The p-value of 0.862 is not significant enough to conclude that an Asian immigrant population makes any difference. Similar statistical analysis on Hispanic/Latino population also revealed there is no statistical significant (p=0.1695) difference between when it comes for Hispanic/Latino population.

TABLE IV. T-TEST ON TOTAL CALLS RECEIVED BASED ON ASIAN IMMIGRANT POPULATION PER STATE

Groups	N	μ	σ	P(T≤t)
> 2.2%	26	29.96	5.95	0.862
≤ 2.2%	25	29.6	8.58	

VII. EVALUATING PHONEYPOT DATA

To demonstrate that Phoneypot provides high quality intelligence about telephony abuse and augments existing datasets, we use completeness, accuracy and timeliness measures discussed in Section I to evaluate the call data captured by it. Completeness and timeliness have the same meaning as described earlier but we need to further explain accuracy. Telephony abuse data may lack accuracy because of two reasons: (1) either the calls included in the data may not be abuse related because they were misdialed by legitimate users, or (2) information about the details of a call may be incorrectly reported or recorded. For example, a timestamp may be incorrectly reported or conflicting opinions may exist about the spam nature of a call. Since Phoneypot only records a call source and destination with a timestamp and no additional details about the call, we need to be concerned about (1) in evaluating accuracy. To decide if sources of calls that came to Phoneypot were fraudulent, we use FTC complaint dataset as the ground truth. We chose this dataset because all reports are complaints (and hence unwanted) and the dataset has been updated continuously for many years. Thus, we use information from the FTC dataset to assess the accuracy of Phoneypot data. We use the same dataset to explore timeliness and completeness. It should be noted that, in the FTC complaint datasets, FTC only provides the source (caller) phone numbers and the reported complaint timestamps (granularity to hour) and not the actual timestamps. Comments and the destination (user) phone numbers were not provided due to privacy reasons.

A. Completeness

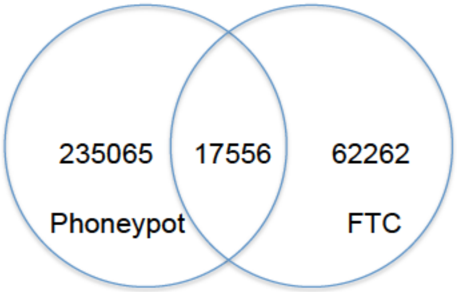


Fig. 9. Overlap of sources reported on FTC which were seen on Phoneypot

Figure 9 shows an overlap of phone numbers that were reported on Phoneypot and on FTC. Our cross checking with the FTC dataset demonstrates that 17,556 of the phone numbers calling our Phoneypot are indeed bad or involved in fraudulent activities. Moreover, these fraudsters are making fraudulent calls to normal people as well as to Phoneypot. 235,065 of the source phone numbers that called Phoneypot were not found in the FTC datasets. This could imply that Phoneypot is able to collect information about fraudulent callers that are not known to other datasets.

TABLE V. T-TEST ON TOTAL CALLS/COMPLAINTS RECEIVED ON PHONEYPOT/FTC RESPECTIVELY

Groups	N	μ	σ	P(T≤t)
Phoneypot	17,756	37.09	411.72	0.0001
FTC	17,756	19.91	209.017	

For the common phone numbers that called both Phoneypot and users who complained to the FTC, we compare the distribution of the total calls from those common numbers in each dataset individually. The difference between the distribution of the complaints reported to the FTC and also the calls coming in to Phoneypot is evident in Figure 10. Based on the t-test analysis shown in Table V, we found that the difference between the two distributions is statistically significant. This demonstrates that Phoneypot not only provides added value to the current intelligence on more source numbers but also on the volume of calls from these sources.

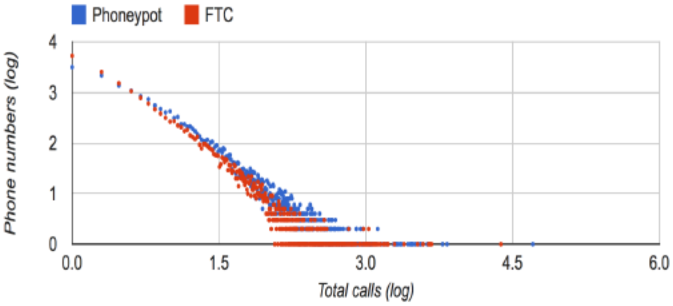


Fig. 10. Call/complaint distribution of the common numbers in each individual datasets.

B. Phoneypot data accuracy

Some of the calls coming to phoneytokens may include misdialed or prank calls. They also include unsolicited abuse calls from spammers, telemarketers, debt collectors etc. At a high level, to assess accuracy, we need to examine the sources of calls coming to Phoneypot and provide evidence that the callers are indeed sources of abuse. For this, we use two features of callers: a) total calls from a source, and b) outdegree – i.e. total number of phoneytokens this source has called. These features are based on the intuition that a legitimate user is unlikely to make a large volume of calls to lot of other phone numbers (some legitimate services may make lots of calls to many phone numbers but they should typically call phone numbers that belong to their customers rather than phoneytokens). Using these feature values, we use X-means clustering algorithm to cluster all these sources (total of 252,621). We set the minimum and maximum clusters to one and the total number of vectors in our dataset, respectively. We choose Euclidean distance for computing similarity between vectors while trying different values for the threshold, in the range (0, 1). Using these settings, we stabilized on 21 clusters.

We then overlaid our evidence from the FTC complaint dataset i.e. 17,556 vectors corresponding to 17,556 common sources (as mentioned in the previous section) to see how they were distributed across the clusters. Interestingly, there were certain clusters where 100% of the source phone numbers were reported on FTC complaint dataset. In contrast, some clusters included a very small percentage of phone numbers reported to FTC, as low as 2.04%. However, in absolute terms, there were only two clusters that had fewer than 20% of their sources reported in the FTC dataset.

Figure 11 shows a small-medium sized cluster with 199 vectors projected to a 2D plot using multi-dimensional scaling. Proximity between vectors on the 2D plot reflects the degree of similarity. 172 of the vectors (in red) were reported on FTC while 27 were not. We examined these 27 and realized

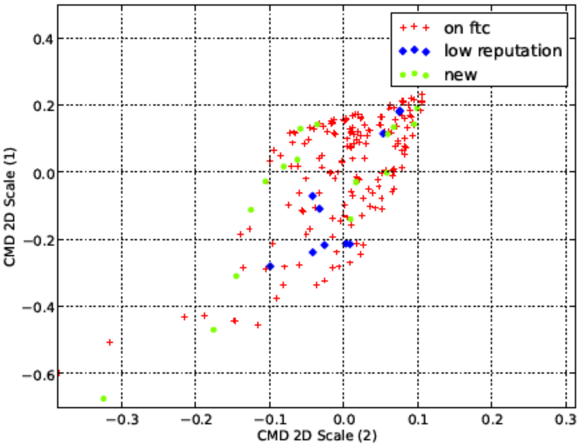


Fig. 11. Example of a cluster with original centroid at (173, 108) where heavy hitting sources other than the ones reported on FTC are seen.

that 10 of them (in blue) had a very low reputation score on the Nomorobo system and 17 (in green) were new to these systems. This shows that using labeled evidence and a feature set, we can gain knowledge about previously unknown sources, which provides evidence that Phoneypot can augment completeness.

Unknown vectors are characterized as abuse sources based on already labeled vectors present in the same cluster. Using this approach, we were able to identify 850 unknown sources that were never reported on FTC but had low reputation on other systems, and 13,812 sources that were positively dubious in interacting with our honeypot but had no trace in any other system. We understand this may not be the best approach to classify unknown sources as malicious but it is a demonstration of the richness of datasets extracted from Phoneypot deployment. We leave it as a future work to conduct an in-depth analysis of the remaining sources after we add recording capabilities to collect additional evidence about the intent of a call.

C. Timeliness

If we revisit our example shown in Section I, we believe there exist several limitations of the crowd source datasets like 800notes and the FTC fraud complaint dataset, one being complaints not being reported in a timely fashion and without accurate call timestamps. In this section, we compare the timeliness of the phone calls received at Phoneypot with ones reported on the FTC fraud complaint dataset.

Figure 12 shows the difference in days when Phoneypot received the calls from the sources before they were reported on FTC. Out of common numbers (17,556) that were reported on FTC, 6,076 (34.6%) phone numbers were reported on Phoneypot earlier than FTC; 4,863 (27.6%) phone numbers were reported on Phoneypot on the same day as on FTC; and 6,6717 (37.6%) phone numbers were reported on FTC before they called Phoneypot. We can observe that phone numbers reported earlier on Phoneypot and FTC are almost equal. It can be argued that Phoneypot did not receive calls first on a significant fraction of the numbers before they were reported on FTC. We understand this observation, however, the user base that reports to FTC fraud complaint database is much larger than the total number of phoneytokens we had for Phoneypot. This also raises another question of how many phoneytokens are enough, and how long Phoneypot should be run. Since we did not run Phoneypot for a long time, we cannot answer this question at this point of time. However, there are phone numbers which were reported on FTC which did not call Phoneypot, therefore one conjecture is that the current pool of phoneytokens is not sufficiently large to have an overall understanding of threats. More phoneytokens can be added to Phoneypot to improve coverage.

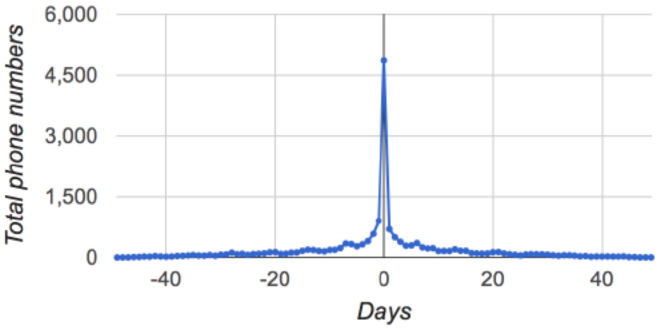


Fig. 12. Timeliness

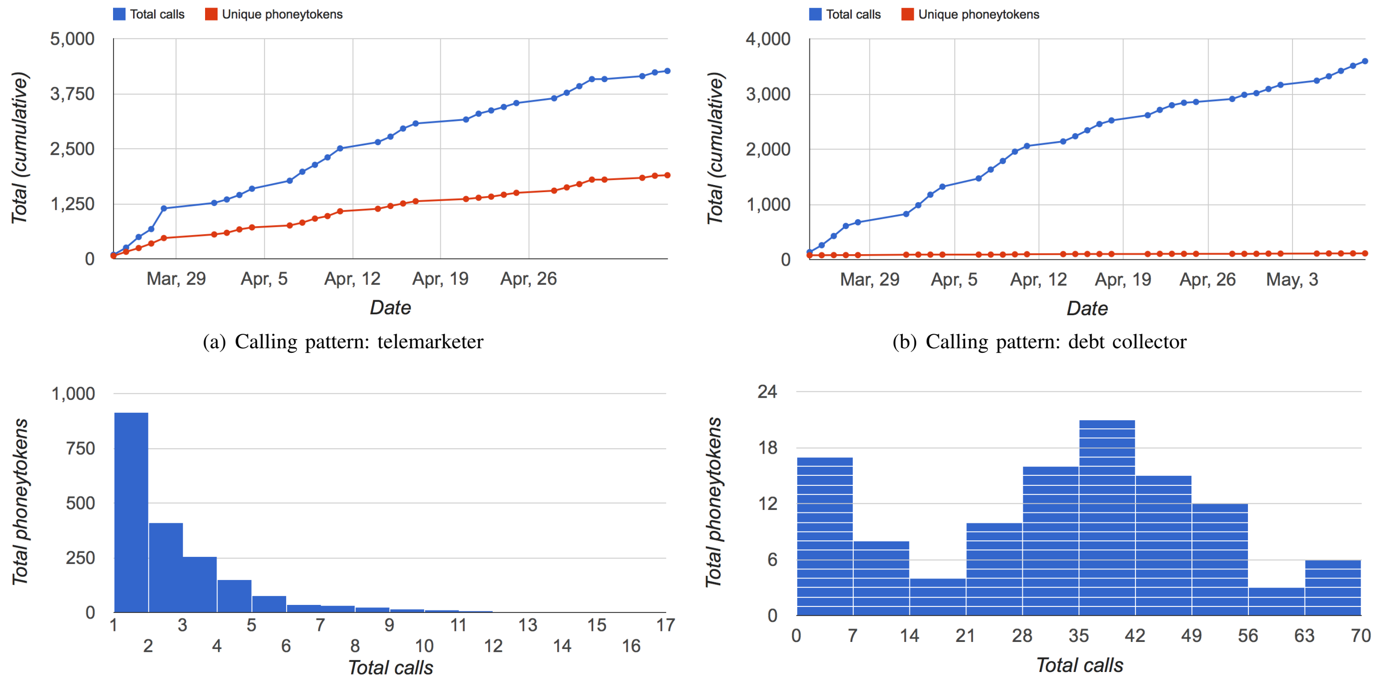
VIII. Detecting Abuse Patterns

In this section, we provide data-driven insights about telephony denial-of-service (TDoS) attacks and other calling patterns that could be indicative of potential abuse. Two key classes of such callers are telemarketers, who make lots of calls to a growing set of targets, and debt collectors, who make persistent and repeated calls to a relatively fixed set of targets. Although neither telemarketing nor debt collections calls are completely illegal, the actions of such callers are regulated in the United States. Many of the aggressive debt collectors and telemarketers often cross the boundary of what is allowed, and their calling patterns could provide evidence of abuse. Based on analysis of Phoneypot data, we provide an example of a fraudulent telemarketing operation.

We manually looked at the top 100 sources that are making a lot of calls. We found evidence of abuse patterns that involve these sources using data collected with Phoneypot. Out of these 100 sources, we found 93 of them were reported on FTC. We were able to obtain some information about these source phone numbers by manually searching them on the web. Table VI shows the classification of these 100 numbers. We could not find information about 36 sources and that is left for future work. Out of the seven sources that were not reported on FTC, there were two that were involved in TDoS attacks, and two of them were debt collectors. We also found one auto-dialer that was repeatedly calling one phoneytoken every 100 seconds within various time windows.

A. Telephony Denial of Service

TDoS attacks generally follow the same model as the more traditional data network denial-of-service – unauthorized users



(a) Calling pattern: telemarketer

(b) Calling pattern: debt collector

(c) Call distribution: telemarketer

(d) Call distribution: debt collector

Fig. 14. Debt collector and Telemarketer calling patterns and call distribution

TABLE VI. CLASSIFICATION OF TOP 100 SOURCES

On FTC		Not on FTC	
Types	N	Types	N
Telemarketer	37	TDoS	2
Debt Collector	18	Debt Collector	2
Political Call	1	Restricted number	1
Survey	1	Spoofed (invalid)	1
Unknown	36	Auto dialer	1
93		7	

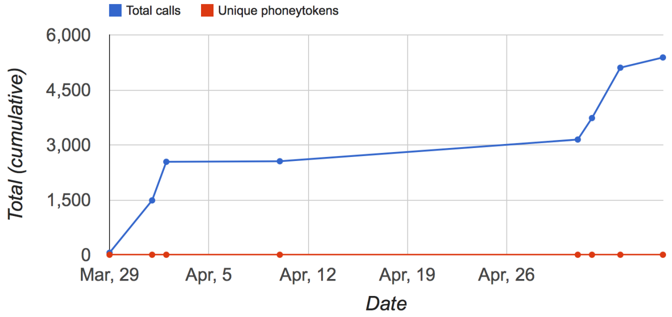


Fig. 13. TDoS attack on a phoneytoken

flood the system with too many access requests and prevent legitimate users from accessing the system. With TDoS, the objective is to make a significant number of phone calls and to keep those calls up for long durations, or to simply overwhelm agent or circuit capacity. The impact on business and revenues can be devastating.

We have seen one such evidence of a TDoS attack from *two* phone numbers on *one* toll-free phoneytoken. Figure 13 shows that there are two time periods when two attack source numbers have made significant number of phone calls within a short span of time to one phoneytoken. There were 1,500 calls made on 30th March 2014 and another 1300 on 31st March. Incidentally, the attacks lasted for two days before reappearing at the end of April. There were only two sources that made all the calls to that particular phoneytoken. Almost all the calls were exactly one minute apart. The two sources that called this phoneytoken were similar looking numbers (ending at 2355 and 2357), giving us an indication that probably these numbers are spoofed. Unfortunately, we could not find out any historical evidence on either source phone numbers or the attack target phoneytoken.

B. Telemarketer and Debt collector

Telemarketing is a method of direct marketing in which a salesperson solicits prospective customers to buy products or services over the phone. A telemarketer tries to cover as many recipients as possible, and hangs up when he figures out that his offer is unlikely to be accepted, which is the most probable case. In contrast, debt collectors are businesses that try to collect payments of debts owned by individuals or businesses and calls are made repeatedly to the same targets.

In Figure 14(a) and 14(b), we show calling patterns of *one* telemarketer and *one* debt collector making calls to phoneytokens. As we can see in Figure 14(a), the total number of calls is increasing with time along with the total unique targeted phoneytokens. This is indicative of telemarketer. Whereas, in Figure 14(b), the total number of calls is increasing but the total targeted unique phoneytokens are constant, indicating a debt collector. Moreover, in telemarketing (see Figure 14(c)), there are fewer calls to more phoneytokens as compared to the case of a debt collector (see Figure 14(d)), where there are more calls to fewer phoneytokens.

We cross checked the source numbers with 800notes database, and based on the complaints we found that the telemarketer is a scam claiming to be "Obama-care health insurance corporation". There were total of 4,266 calls made by this number to the phoneytokens, however, there were only 186 complaints being reported on FTC during the same period. We also found that the debt collector pattern source number belongs to Allied Interstate, which is a debt collector that has been fined 1.75 million USD in 2010 [28] by the FTC for illegal practices. There were total of 3,768 calls made by this number to the phoneytokens, however, there were only 89 complaints being reported on FTC during the same period. The significantly higher number of calls in these patterns in Phoneypot data makes it easier to detect these frauds.

IX. Discussion and Limitations

As we mentioned, the experiments reported in this paper present early results that help to gain insights into the effectiveness of a telephony honeypot. We have not covered any of the possible options to seed the phoneytokens and not deployed the telephony honeypot in all possible manner as mentioned in the paper. We leave this for future work. Caller ID spoofing is another thrust area which can impact the accuracy and performance of a telephony honeypot. It has been explored in other research [52] and we do not address caller ID spoofing problem in this paper. As with other security research, the goal of threat information collection and analysis is to develop defenses that can help contain these threats. We need to do the same with the intelligence that can be derived from Phoneypot. We will explore several options, ranging from associating reputation with phone numbers similar to IP and domain name reputation, and black and whitelists of phone numbers. However, spoofing of phone numbers is much easier and has been detected. Our future work will address how best to utilize Phoneypot intelligence to detect such spoofing.

X. Conclusion

Cyber criminals are now using vulnerabilities in the IP telephony ecosystem to craft attacks that use legitimate sounding phone calls to scam users. Such incidents are increasing at an alarming rate. There exist self-reported fraud complaint databases of unsolicited calls like 800notes and the FTC's complaint datasets. However, in this paper, we demonstrate the need to enhance such databases to address problems such as delay between when the actual fraud call date & time and when the complaint was registered, lack of intelligence and the accuracy of the reports due to inclusion of other abuse like email spam reports that corrupt the datasets.

We explored the feasibility of using a honeypot to collect better intelligence about telephony attacks. We propose Phoneypot, a first and the largest telephony honeypot and demonstrate a concrete implementation for it. Such a telephony honeypot must address several new challenges and we introduce phoneytokens to illustrate them. We also report experiences with 39K phoneytokens that were deployed and data collected over a seven week period. Phoneypot received more than 1.3M unsolicited calls. We were able to investigate and validate some of these calls with FTC complaint datasets and a proprietary database from robocall blocking service provided by Nomorobo. We also found that older block of numbers tend to receive more calls as compared to newer block of numbers. We also observed evidence of abuse patterns including debt collector and telemarketing calls patterns. We have seen clear evidence of telephony denial of service attacks. Finally, we compared the timestamps of phone numbers reports on FTC fraud complaint database and found that there were many instances where Phoneypot received calls from fraudulent phone numbers before it was reported on the FTC dataset. This shows that Phoneypot can be used to complement current data collection mechanisms related to telephony abuse.

Many issues related to telephony threats remain to be explored. In future, we will explore seeding of phoneytokens as well as defenses against various threats.

Acknowledgement

This research was supported in part by National Science Foundation award 1318167. Any opinions, findings and conclusion or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

[1] "419 Scam Directory," http://www.419scam.org/.

[2] "Asterisk," http://www.asterisk.org/.

[3] "Cisco 8-Port Channelized T1/E1 Shared Port Adapter," http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/shared-port-adapters-spa-interface-processors/product_data_sheet0900aecd8027ca10.html.

[4] "Decline of landline in India," http://telecomtalk.info/decline-of-landline-in-india/66093/.

[5] "Directory of Unknown Callers," http://800notes.com/.

[6] "FreeSWITCH," https://www.freeswitch.org/.

[7] "FTC Action Halts Debt Relief Marketing Operation," http://www.ftc.gov/opa/2012/09/nelsongamble.shtm.

[8] "FTC Halts Massive Tech Support Scams," http://ftc.gov/opa/2012/10/pecon.shtm.

[9] "FTC Leads Joint Law Enforcement Effort Against Companies That Allegedly Made Deceptive Cardholder Services Robocalls," http://ftc.gov/opa/2012/11/robocalls.shtm.

[10] "FTC Shuts Down Robocall Operation That Allegedly Claimed to Help Consumers Get FTC Consumer Refunds," http://www.ftc.gov/opa/2012/12/cubanexchange.shtm.

[11] "H.323 and SIP Integration," http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a0080092947.shtml.

[12] "Hi, this is Rachel from RoboCaller services calling. Press 1 to be scammed." http://arstechnica.com/tech-policy/2012/11/hi-this-is-rachel-from-robocaller-services-calling-press-1-to-be-scammed/.

[13] "Honeytokens: The Other Honeypot," http://bandwidthco.com/sf_whitepapers/honeypots/Honeytokens%20-%20The%20Other%20Honeypot.pdf.

[14] "Huawei E220," http://www.huaweie220.com/.

[15] "International Revenue Share Fraud: Are We Winning the Battle Against Telecom Pirates?" http://bswan.org/revenue_share_fraud.asp.

[16] "Missed Call From A Mystery Number? Be Careful." http://techcrunch.com/2014/02/02/missed-call-scam/.

[17] "Multinational Crackdown on Computer Con Artists," http://www.nytimes.com/2012/10/04/business/multinational-crackdown-on-computer-con-artists.html?_r=0.

[18] "PENAL CODE SECTION 630-638 ," http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=630-638.

[19] "Publication of FTC accounts data 2012/13," http://data.gov.uk/dataset/publication-of-ftc-accounts-data-2012-13.

[20] "Swindlers Use Telephones With Internets Tactics," http://www.nytimes.com/2014/01/20/technology/swindlers-use-telephones-with-internets-tactics.html.

[21] "Tropo," https://www.tropo.com.

[22] "Twilio," http://www.twilio.com.

[23] "The vishing guide." http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf.

[24] "VoIP Honey," http://voiphoney.sourceforge.net/.

[25] "Wangiri Fraud." http://www.xintec.com/wangiri-fraud/.

[26] "Watch Out For a 'One Ring' Cell Phone Scam," http://boston.cbslocal.com/2014/02/04/better-business-bureau-watch-out-for-one-ring-cell-phone-scam/.

[27] "Wireless Honeypot Countermeasures," http://www.symantec.com/connect/articles/wireless-honeypot-countermeasures.

[28] "Debt Collector Will Pay $1.75 Million to Settle FTC Charges," http://www.ftc.gov/news-events/press-releases/2010/10/debt-collector-will-pay-175-million-settle-ftc-charges, 2010.

[29] "United States Census Bureau," http://www.census.gov/popclock/, 2010.

[30] "Area-Codes.com," http://www.area-codes.com/, 2014.

[31] "Listen to the largest ever phone scam involving IRS impersonators," http://www.washingtonpost.com/blogs/federal-eye/wp/2014/04/16/listen-the-largest-ever-phone-scam-involving-irs-impersonators/, 2014.

[32] W. Aiello, F. Chung, and L. Lu, "A random graph model for massive graphs," in *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, ser. STOC '00. New York, NY, USA: ACM, 2000, pp. 171–180.

[33] Y. Bai, X. Su, and B. Bhargava, "Detection and filtering spam over internet telephony: a user-behavior-aware intermediate-network-based approach," in *Proceedings of the 2009 IEEE international conference on Multimedia and Expo*, ser. ICME'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 726–729.

[34] V. Balasubramaniyan, M. Ahamad, and H. Park, "CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation," in *CEAS'07*, 2007, pp. –1–1.

[35] V. 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.

[36] A. Costin, J. Isacenkova, M. Balduzzi, A. Francillon, and D. Balzarotti, "The role of phone numbers in understanding cyber-crime schemes," in *PST*, 2013, pp. 213–220.

[37] D. Dagon, X. Qin, G. Gu, W. Lee, J. B. Grizzard, J. G. Levine, and H. L. Owen, "HoneyStat: Local Worm Detection Using Honeypots." in *RAID*, ser. Lecture Notes in Computer Science, E. Jonsson, A. Valdes, and M. Almgren, Eds., vol. 3224. Springer, 2004, pp. 39–58.

[38] R. do Carmo, M. Nassar, and O. Festor, "Artemisa: An open-source honeypot back-end to support security in VoIP domains." in *Integrated Network Management*, N. Agoulmine, C. Bartolini, T. Pfeifer, and D. O'Sullivan, Eds. IEEE, 2011, pp. 361–368.

[39] D. Endler and M. Collier, *Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions*, 1st ed. New York, NY, USA: McGraw-Hill, Inc., 2007.

[40] S. E. Griffin and C. C. Rackley, "Vishing," in *Proceedings of the 5th Annual Conference on Information Security Curriculum Development*, ser. InfoSecCD '08. New York, NY, USA: ACM, 2008, pp. 33–35.

[41] J. Isacenkova, O. Thonnard, A. Costin, A. Francillon, and D. Balzarotti, "Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations," *EURASIP Journal on Information Security*, vol. 2014, no. 1, p. 4, 2014.

[42] N. Jiang, Y. Jin, A. Skudlark, W.-L. Hsu, G. Jacobson, S. Prakasam, and Z.-L. Zhang, "Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis," in *Proceedings of the 10th international conference on Mobile systems, applications, and services*, ser. MobiSys '12. New York, NY, USA: ACM, 2012, pp. 253–266.

[43] N. Jiang, Y. Jin, A. Skudlark, and Z.-L. Zhang, "Greystar: Fast and Accurate Detection of SMS Spam Numbers in Large Cellular Networks Using Grey Phone Space," in *Proceedings of the 22Nd USENIX Conference on Security*, ser. SEC'13. Berkeley, CA, USA: USENIX Association, 2013, pp. 1–16.

[44] ——, "Understanding SMS Spam in a Large Cellular Network: Characteristics Strategies and Defenses," in *RAID*, 2013, pp. 328–347.

[45] J. P. John, F. Yu, Y. Xie, A. Krishnamurthy, and M. Abadi, "Heat-seeking Honeypots: Design and Experience," in *Proceedings of the 20th International Conference on World Wide Web*, ser. WWW '11. New York, NY, USA: ACM, 2011, pp. 207–216.

[46] A. D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research." *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 514–537, 2012.

[47] J. G. Levine, J. B. Grizzard, and H. L. Owen, "Using Honeynets to Protect Large Enterprise Networks," *IEEE Security and Privacy*, vol. 2, no. 6, pp. 73–75, Nov. 2004.

[48] A. Litan, "U.S. Banks Are Improving Much Needed Online Security, but Their Phone Channels Need More Attention," Gartner Survey, Tech. Rep. G00219646, Nov 2011.

[49] F. Maggi, "Are the Con Artists Back? A Preliminary Analysis of Modern Phone Frauds," in *Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology*, ser. CIT '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 824–831.

[50] B. Mathieu, S. Niccolini, and D. Sisalem, "SDRS: A Voice-over-IP Spam Detection and Reaction System," *IEEE Security and Privacy*, vol. 6, no. 6, pp. 52–59, 2008.

[51] I. Murynets and R. Piqueras Jover, "Crime Scene Investigation: SMS Spam Data Analysis," in *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, ser. IMC '12. New York, NY, USA: ACM, 2012, pp. 441–452.

[52] H. Mustafa, A.-R. Sadeghi, S. Schulz, and W. Xu, "You can call but you can't hide: Detecting caller id spoofing attacks," in *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2014.

[53] M. Nassar, R. State, and O. Festor, "VoIP Honeypot Architecture." in *Integrated Network Management*. IEEE, 2007, pp. 109–118.

[54] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-time," in *Proceedings of the 7th Conference on USENIX Security Symposium - Volume 7*, ser. SSYM'98. Berkeley, CA, USA: USENIX Association, 1998, pp. 3–3.

[55] A. Pitsillidis, C. Kanich, G. M. Voelker, K. Levchenko, and S. Savage, "Taster's choice: A comparative analysis of spam feeds," in *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, ser. IMC '12. New York, NY, USA: ACM, 2012, pp. 427–440.

[56] T. H. Project, "Know Your Enemy: Defining Virtual Honeynets," http://old.honeynet.org/papers/virtual/.

[57] N. Provos, "A virtual honeypot framework," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04. Berkeley, CA, USA: USENIX Association, 2004, pp. 1–1.

[58] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, 1st ed. Addison-Wesley Professional, 2007.

[59] 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*, ser. Lecture Notes in Computer Science, A. Pras and M. van Sinderen, Eds., vol. 4606. Berlin: Springer Verlag, July 2007, pp. 70–77.

[60] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, "Detecting SPIT Calls by Checking Human Communication Patterns." in *ICC*. IEEE, 2007, pp. 1979–1984.

[61] A. Ramachandran and N. Feamster, "Understanding the Network-level Behavior of Spammers," in *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ser. SIGCOMM '06. New York, NY, USA: ACM, 2006, pp. 291–302.

[62] M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," in *Proceedings of the 13th USENIX Conference on System Administration*, ser. LISA '99. Berkeley, CA, USA: USENIX Association, 1999, pp. 229–238.

[63] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner, “SPam over Internet Telephony (SPIT) Prevention Framework.” in *GLOBECOM*. IEEE, 2006.

[64] D. Shin, J. Ahn, and C. Shim, “Progressive multi gray-leveling: a voice spam protection algorithm.” *IEEE Network*, vol. 20, no. 5, pp. 18–24, 2006.

[65] L. Spitzner, *Honeypots: Tracking Hackers*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002.

[66] S. Staniford, V. Paxson, and N. Weaver, “How to Own the Internet in Your Spare Time,” in *Proceedings of the 11th USENIX Security Symposium*. Berkeley, CA, USA: USENIX Association, 2002, pp. 149–167.

[67] C. Valli and M. A. Lawati, “Developing VoIP Router Honeypots.” in *Security and Management*, H. R. Arabnia, K. Daimi, M. R. Grimaila, G. Markowsky, S. Aissi, V. A. Clincy, L. Deligiannidis, D. Gabrielyan, G. Margarov, A. M. G. Solo, C. Valli, and P. A. H. Williams, Eds. CSREA Press, 2010, pp. 615–619.

[68] G. Zhang and S. Fischer-Hübner, “Detecting near-duplicate SPITs in voice mailboxes using hashes,” in *Proceedings of the 14th International Conference on Information Security*, ser. ISC’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 152–167.