Centralized Spam Over Internet Telephony (SPIT) Control on VoIP

Haider Jarral, Farrukh Mehmood, Afif Ali

Department of Electrical Engineering and Computer Science, Wichita State University, Kansas, USA

Abstract- Voice over IP is becoming increasingly a valid alternative to traditional telephony networks because of its low cost, higher flexibility and easy integration. On the other hand Spam over IP Telephony (SPIT) is increasing because of the same vey benefits. There have been numerous proposals in regard to prevention of SPIT however it is very difficult to place a call under the category of SPAM or not on the basis of computations since it totally relies on the uneasiness caused to the end user. Black Listing and Grey Listing are well known methods in SPIT prevention which is based on analyzing call detail records. This paper proposes a method of controlling the SPAM centrally through a server based on Grey Listing and Black Listing recording SPAM flag based on the digits entered by end user on the termination or during the call.

I. Introduction

Increasing popularity of VoIP has made it a valid alternative for traditional telephone setups for corporate environments. The ease of setup, flexibility of usage and lesser cost has made it very popular among multinational setups. At the same time the same very features are misused by companies for their own benefits. Besides all other security threats Spam Over Internet Telephony (SPIT) is one of the popular method used for advertising business through phone using VoIP. The attackers use the low cost feature of VoIP to exploit this security threat. SPIT in other words is similar to spam emails on internet. In email spamming a victim receives dozens of irrelevant emails used for marketing or other purposes. If SPIT attacks are not controlled and VoIP keeps on expanding as valid alternative it may result in continuous ringing of phones in a corporate environment similar to email spamming i.e. email arriving every minute or so.

II. Types of SPIT Attacks

Telemarketing

It is one of the most common attacks that occur on VoIP environments. Surveys [1] suggest that an average American receives 2 to 3 calls minimum each day targeted for telemarketing. Telemarketers target victims of a particular domain or business for acquiring there services or products. VoIP has enabled many companies to open off shore offices to run such telemarketing campaigns at very low cost.

Call Bots

Call bots are somewhat similar to telemarketers except the fact that calls are generated by computers or pre recorded machines and they utilize a pre defined list of numbers and message is typically the same throughout.

III. Existing Countermeasures for SPIT

Different techniques and algorithms have been designed to control SPIT attacks [2][3][4] however each has its pros and cons. Below is a brief overview of the existing techniques.

Blacklist and Whitelist Filtering: This method compares the identity of a caller with a pre-defined list of identities, if the number is in the whitelist the call is allowed otherwise the call is dropped. The numbers in the black list are known as malicious callers and number in white list are known as trusted callers.

Greylisting: If a user calls for the first time his number is put into a temporary list called grey list and immediately after that caller is said to call again if he does, it is placed in the white list otherwise it is placed in black list.

SIPFW: SIP Firewall is implemented in this method. It uses a fingerprinting model. Active Fingerprinting creates SIP messages manually to obtain specific answers. Passive Fingerprinting does not make any changes to existing message.

Content Filtering: This method was originally designed for spam email filtering. In VoIP it requires speech recognition which involves significant computations.

User Reputation: This method is applied by the VoIP Service Provider (VSP). Each VSP maintains Call Detail Records (CDR) data of its users and analyze them basing on the SPAM index. If the caller crosses the index the call is blocked.

Pattern Anomaly Detection: This method uses probabilistic model of call arrival and algorithm defines if the incoming call is SPIT or not. It is based on statistical data and deterministic models.

Turing Test: This method asks caller a question if the answer is correct the call is allowed. This method is not very successful in case of telemarketers however is works fine with call bots.

Call Rate: This method checks the calling frequency of a caller if it's more than certain limit the call is blocked otherwise it goes through.

Problems with existing methods

Since all the existing methods require significant computations during the checking process and an authentic caller may not like such delay to pass through the security check. Similarly sometimes computations may result in error since spam in case of VoIP is totally based on users consent. Some calls may actually be spam calls but after callee has received the call, it may not be spam anymore. Similarly there might be scenarios

where a same call is spam for one user and same call is not a spam for another user. Call bots can be placed under the category of SPAM calls for all users but in case of telemarketing some users may like to know about promotional updates and better offers from other companies and some user may not like it at all. Nevertheless marking call as SPAM or not is based on the end users consent.

Existing methods do not allow any such ability to the end user to mark the call as SPAM. Consent Based [5] method is still under standardization by Internet Engineering Task Force (IETF). Using user consent would significantly reduce the computations involved thus reducing the delay in call setup.

IV. Consent Based Spam Marking Model

This method is simple and does not involve many computations or algorithms. It requires all calls to be routed through the central server (IP Private Branch Exchange - IP PBX) which already exists in most of the corporate environment based on VoIP. Once the call is established, the session is monitored for any Dual Tone Multiple Frequency (DTMF) from the end user. If any DTMF is detected it is evaluated on the basis of value assigned to it in server. DTMF can only be either the two cases discussed below.

- SPAM Mark: If end user presses the key defined to mark SPAM then the caller will be marked as SPAM. This could be defined in company policy and can be different for different companies. In our model we use digit 1 as SPAM Mark.
- Not SPAM Mark: If end user presses the key defined to no SPAM mark then the caller will be marked as legit caller. This digit could vary from company to company. In our model we use digit 0 as no SPAM Mark.

A sample model is illustrated below in Figure 1.

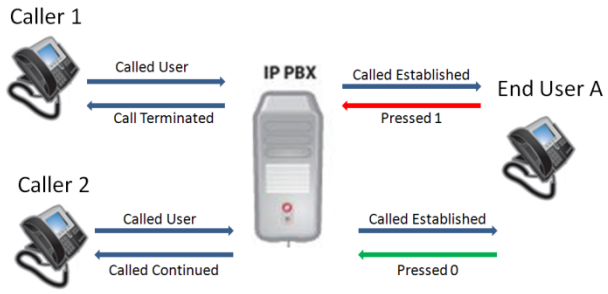

Figure 1. Simple feedback for two different callers

Fig. 1 shows a simple feedback collected from end user for two different callers. End User A has marked caller 1 as SPAM and caller 2 as no spam. While the end user marks a caller with SPAM or NO-SPAM a flag table is maintained at server for both the callers as shown.

Caller	Status	Reported By	Count
Caller 1	SPAM	End User A	1
Caller 2	NOT- SPAM	End User A	1

Table 1. SPAM list table

Table 1 is maintained at servers end and used for filtering the calls when a user calls again. Each SPAM is recorded against the user who reported it as SPAM. This would ease the issue of one caller SPAM for one user and NOT-SPAM for another user. Count keeps the track of each number reported SPAM how many times with time stamp.

Depending on the number of users in an organization a threshold level can be defined for SPAM index. If 10% of the users report the number as SPAM it is marked as SPAM or otherwise as per company policy. Call bots can be determined more quickly since they use a sequential series of number listings. If a call is reported 3 times within 5 minutes, the caller is a computer generated message since it is using a list of sequential numbers. Same scenario stays true for the telemarketers too. If a telemarketer is trying to make calls in the same organization at different numbers and is reported SPAM by 3 users he'll be flagged as SPAM.

Once the user marks the number as SPAM the caller is redirected to pre-recorded message stating that his number has been marked as SPAM if he considers this an error he should contact the network administrator of the company.

There could be scenarios in which user forgets to give feedback for the call. In those cases if the called number already has the feedback in the SPAM list table then nothing is done but if that's not the case server initiates call back to end user requesting feedback of the latest call received by him.

The method of SPAM list table reduces the need of two separate lists, white list and black list [5]. One single list is used to scan all incoming calls. If the call has SPAM flag marked lower than 10% the call is allowed if not the call is redirected to pre-recorded message. Let's see how incoming calls are scanned in VoIP environment.

V. SIP Protocol in VoIP

Session Initiation Protocol (SIP) is an application layer protocol most widely used to create, maintain and terminate multimedia sessions. SIP supports five different types of services namely: User availability, User location, User capabilities, Session setup and Session management. Different components used by SIP are:

UAC (User Agent Client) – client that starts the signalling
UAS (User Agent Server) – Server that responds to agent
Proxy Server – receives connection request and forwards them if end user is not in its domain
Redirect Server – Sends the destination information to the requester
Location Server – receives registeration request and updates its database

A look at SIP packet structure will help us determine how incoming calls can be analysed. Below is a sample SIP request[6] for initiating a call:

INVITE sip:user@sipserver.com SIP/2.0
(Message Headers)

Via: SIP/2.0/UDP 10.10.10.10:5060
From: "Me" <sip:me@sipserver.org>;tag=a0
To: "User" <sip:user@sipserver.org>
Call-ID: d@10.10.10.10
CSeq: 1 INVITE
Contact: <sip:10.10.10.10:5060>
User-Agent: SIPTelephone
Content-Type: application/sdp
Content-Length: 251
(Message Body)
v=0
o=audio1 0 0 IN IP4 10.10.10.10
s=session
c=IN IP4 10.10.10.10
m=audio 54742 RTP/AVP 4 3
a=rtpmap:4 G729/8000
a=rtpmap:3 GSM/8000

The *From* field clearly indicates the origin of call. Our main concern is with this field. All incoming calls are routed through the SPAM list table. The SIP identity of incoming caller is stripped from the message header and matched with the Caller field in the table. Below is the priority of incoming calls analysis using SPAM Table:
IF Status = Nil
(Call is allowed, feedback call generated after call)

IF Status=NOT_SPAM and Count > 0
(The call is allowed)

IF Status= SPAM and Count < 10
(The call is allowed)

IF Status=NOT_SPAM Count > 0 AND Status = SPAM Count > 0
(If *To* Field in message header matches the destined user who marked it NOT_SPAM the call is allowed otherwise it is blocked)

IF Status= SPAM Count > 9
(Call is blocked)

IF Status= SPAM and Count > 2 where Last Count – Present Count = updated in less than 90 secs
(Call is blocked)

The above mentioned statements cover almost all the scenarios discussed in section V. These statements are written considering the SPAM Index value to be 10. All the incoming calls whose SPAM index is 10 will be blocked. SPAM index can be a variable value set by network administrator.

VI. Centralized Control

All the numbers that cross the SPAM index are reported to VSP on periodical basis. A black list is maintained at VSP if let's say 5 organization report the number is SPAM it should be black listed and stopped from making any further calls. However a warning should be issued when the number is reported each time so that organization may stop SPIT. This would enable the calls to be blocked right after they originate and reach their VSP. This centralized control will enable better control of SPIT. Once the VSP receives the number reported as black list, VSP can also send the number to other VSP's for monitoring. That will enable more quick marking of SPIT callers.

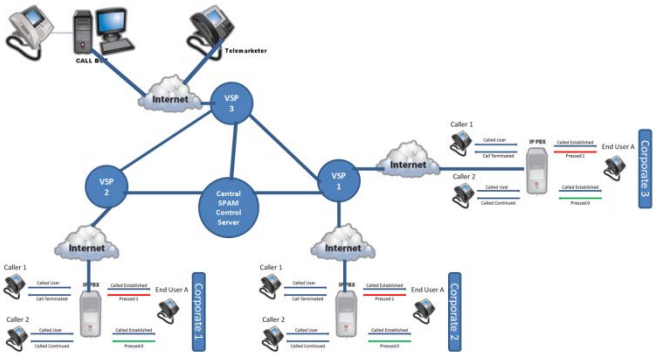

Figure 2. Central Server to Control SPIT

The Fig. 2 shows a central SPAM Control Server, which is maintaining list of all blacklisted numbers reported by all VSP's. It also sends the update of blacklisted number from one VSP to other VSPs and once they also confirm it as SPAM caller that number is sent to all VSP's marking it as SPIT. This central control will even enable to control the SPIT at a global level since all SPAM numbers are reported to a central server.

VII. Conclusion

Though SPIT hasn't gain significant importance in market yet, but if VoIP keeps on expanding at its current rate, so will SPIT and it might become similar as email spamming. The concept of central server can control SPIT attacks significantly but it might come with a slight disadvantage of delay in call setup though very lesser than traditional scanning techniques. But again if the situations in which a corporate is receiving SPIT call at a high rate a little delay in analyzing the call is better than wasting few minutes and bugged by a call bot or telemarketer. And central server may grow effectively with time in controlling the SPIT since the reported numbers will be maintained and updated periodically. And the method still holds good for people who still want to receive the promotional offers.

Acknowledgment

The paper has been written studying the options and features available with open source VoIP software Asterisk.

References

[1] Telemarketing Statistics – Diana Mey. http://www.dianamey.com/telemarketing-statistics/

[2] TaiJIN Lee, et al, User Reputation based VoIP Spam Defense Architecture Korea Information Security Agency Seoul Womern University

[3] Juergen Quittek, Saverio Niccolini, Sandra Tartarelli, and Roman Schlegel, NEC Europe Ltd., On Spam over Internet Telephony (SPIT) Prvention IEEE Communications Magazine, August 2008

[4] G.F. Marais, et al. SIP Vulnerabilities and Anti-SPIT Mechanism Assesment, information Security and Critical Infrastructure Protection Research Group, IEEE, 2007.

[5] Scatá, M.; Corte, A.L.; , "Security analysis and countermeasures assessment against spit attacks on VoIP systems," *Internet Security (WorldCIS), 2011 World Congress on* , vol., no., pp.177-183, 21-23 Feb. 2011

[6] SIP packet Structure - http://www.voipmechanic.com/sip-basics.htm

AUTHORS

First Author – Haider Jarral, Department of Electrical Engineering and Computer Science, Wichita State University, Kansas, USA, hkjarral@wichita.edu
Second Author – Farrukh Mehmood, Department of Electrical Engineering and Computer Science, Wichita State University, Kansas, USA, fxmehmood@wichita.edu
Third Author – Afif Ali, Department of Electrical Engineering and Computer Science, Wichita State University, Kansas, USA, axali1@wichita.edu