Mitigating SPIT (VOIP Spam) as an Antispam Technique

Darshana Prajapati[1] Girish Khilari[2]
[1]Gujarat Technological University PG School, Ahmedabad, Gujarat, India
[2]MS (Software Systems), BITS Pilani

Abstract— Nowadays we are getting various calls disturbing our day-to-day activities. The current example may include the bank calls that we are getting for taking various loans likes students purpose, business purpose and other purpose and whatsoever reason as we are not concerned with it. So there should be some unique method or the combination of the various Antispam techniques and this combination can be used to mitigate or reduce the spam calls or we can say Spam over Internet Telephony (SPIT). There are usually many Antispam techniques available that can be used but in this paper the main techniques that we are going to work are as follows: (1) Grey listing and (2) Handshaking/Challenge/Turing test. The combination that we are doing is with the grey list method with the Handshaking/Challenge/Turing tests. Once the user passes the Turing test he will be passed through the grey listing method and finally a decision will be made whether a call is spam or not. The main objective of this paper will be to analyse the techniques and find out the best possible combination of the techniques to Mitigate SPIT.

Keywords— SPIT, VOIP Spam, SIP, Prevention mechanism, Antispam Techniques.

I. INTRODUCTION

Internet telephony has gained much popularity as an easy way to communicate and make calls to distant places through the internet. It provides a feature of free telephone calls to be made with their software anywhere in the world[1]. These internet telephony products are sometimes called VOIP products. Like e-mail spam, voice spam also called SPIT (Spam over Internet Telephony) is a common misuse of VOIP products and services that transfer bulk messages to phones through internet and broadcasted through VOIP [2]. This research aims at developing a modular framework for SPIT detection and prevention.

Since it makes use of the ubiquitous IP protocol, Voice over Internet Protocol (VoIP) has become a leading technology used in implementing voice services over data networks[1]. Businesses are increasingly switching over to VoIP systems. Frost and Sullivan, a marketing research firm, recently estimated the annual growth rate for IP enabled telephone equipment to be 132%.Additionally, it is estimated that 70% of Fortune 1000 companies use VoIP in their network structure. The main difference between the email spam and voip spam is that, in email spam, whenever the spam mail comes the user will not be disturbed because he will get the mail at midnight without any disturbance, whereas in the case of voip spam, even in the midnight if the spam call comes then the user will be disturbed for receiving the calls, the problem of Spam over Internet Telephony is likely to increase in the future[8].

To identify SPIT calls we have introduced here a framework with multiple modules, which will identify these calls with the help of a some antispam methods, like Turing test, Grey listing, Memory bound functions[1] .We have placed an anti-SPIT server in between the SIP (Session Initiation Protocol) proxy and the VoIP gateway so that every call passes through it and only a call passing the tests can reach VoIP server and thus call the receiver.

II. SPAM OVER INTERNET TELEPHONY (SPIT)

VoIP spam or SPIT (Spam over Internet Telephony) are bulk unsolicited, automatically dialed, pre-recorded phone calls using the Voice over Internet Protocol (VoIP). Telephone spam is comparable to E-mail spam, but due to its synchronous character, different mitigation methods are needed.[1]

The main technology that usually VoIP uses is Session Initiation Protocol (SIP). This technology has received significant support from most major telecommunication vendors, and is showing signs of becoming the industry standard for voice, video and other interactive forms of communication such as instant messaging and gaming.

VoIP is a packet switched network and is vulnerable to different security threats that include: social threats, traffic attacks, denial of service attacks, and service abuse attacks from malicious users [1]. For SPIT callers, VoIP is a cost effective way to re-utilize the email Spam generation architecture and send a massive number of Spam voice messages. The SPIT caller generates SPIT calls for advertising their products, getting callee credit card information, making callee to dial special expensive numbers, and generally Voice phishing (Vishing).

Currently, three different types of VoIP spam forms have been recognized [9]: (a) Call SPIT, which is defined as bulk, unsolicited session initiation attempts in order to establish a multimedia session, (b) Instant Message SPIT, which is defined as bulk, unsolicited instant messages and it is well known as SPIM, and (c) Presence SPIT, which is defined as bulk, unsolicited presence requests so as the malicious user to become a member of the address book of a user or potentially of multiples users.

III. STEPS OF SPIT

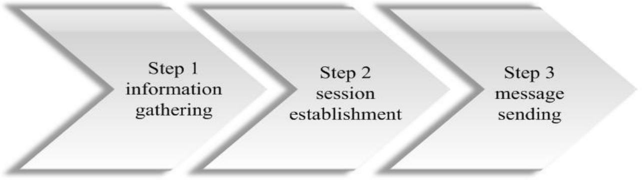

Fig 3: 3 Main Steps of SPIT

Dr. Andreas [3] presented a SPIT goal to establish a communication session with as much victims as possible in order to transfer a message to any available endpoint. The attacker can ful_l this via three steps. First the systematic gathering of the contact addresses of victims. Second is the establishment of communication sessions with these victims and the third step is the sending of the message.
SPITers attack the legitimate users in 3 steps as follows:

A. STEP 1: Information gathering: If an attacker wants to reach as many victims as possible he must catalogue valid assigned SIP URIs. The premises for the Scan attack are the possession of at least one valid account and knowledge about the scheme of SIP URIs of the targeted platform.

B. STEP 2: Session establishment: When the attacker has collected all the information about the users that are registered into the server they try to establish the session between the caller and make an attack on the users. So the legitimate user is not aware of the attack that are happening to them.

C. STEP 3: Message Sending: The last step of the SPIT process is the media sending after the session has been established. Which type of media is sent, depends on the scenario in which the SPIT attack takes place. The best scenario classification can be found and defines three types of SPIT scenarios: Call centres, Calling bots, Ringtone Spit. An adaption of this method could be a SPIT attack where the attacker just wants to let the victim’s phone ring, in order to disturb the victim. In this special case no media is sent at all and the session is terminated as soon as the phone rings (e.g. when a "180 Ringing" is received). Obviously this is the most annoying facet of SPIT.

IV. REFERENCE MODEL FOR SPIT PREVENTION A

A. THREE STAGES OF SPIT PREVENTION

1) STAGE 1: NO INTERACTION WITH CALL PARTICIPANTS WHITELISTING, BLACKLISTING

Whitelisting is a technique primarily used in instant messaging networks. In case of VoIP a whitelist contains the telephone numbers of the people that are allowed to call you. When anyone whose telephone number is not on the whitelist tries to call you he is blocked. [6] Whitelists are not as easy to circumvent as other VoIP spam protection techniques, because a change of identity of the spammer will not work to circumvent a whitelist.

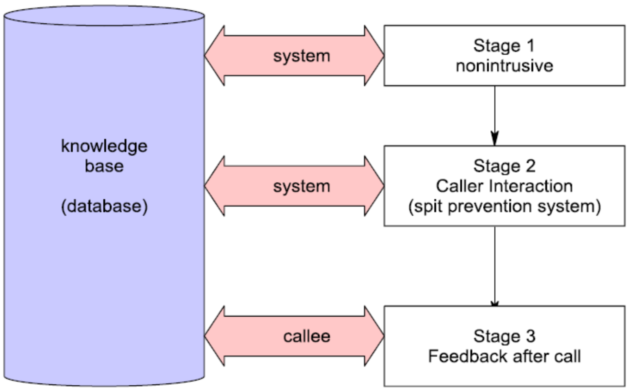

Fig 4: Reference Model for SPIT Prevention

– *BLACKLISTING*

The complete opposite of whitelisting, as discussed in the previous section, is blacklisting. [6]Instead of maintaining a list of the phone numbers of the people that are allowed to call you, you maintain a list of the phone numbers of people that are not allowed to call you. A blacklist specifies who is to be kept out allowing all others to pass test.[5]
For example , when a SIP call comes from a SIP source the detection gateway tries to find and entry to this SIP source in its white list. If a such entry exits then the call is transferred otherwise it looks for an entry to this SIP source in its blacklist[5].

2) STAGE 2: CALLER INTERACTION GREYLISTING:

Greylisting is based on a simple rule that is applied to all incoming calls: each incoming call will be blocked unless the same SIP URI has tried to establish a call within the last N hours/minutes[1]. When the sender is blocked, he will receive a message like “the user is currently busy”. Normal users will then try to call back later. After the sender has called back his SIP URI is added to the whitelist and all future calls will be connected immediately

A grey list contains addresses of callers that should be blocked on its first attempt and later allowed if a second attempt is made within a specific time window thus increases number of attempts to reach called. [13]

– *MEMORY BOUND FUNCTION:*

The basic idea of Memory bound functions is: “If I don’t know you and you want to send me a message, then you must prove that you spent, say, ten seconds of CPU time, just for me and just for this message”. This “proof of effort” is mainly cryptographic, it’s hard to compute but very easy to check.

Memory Bound Function is following way: it accept the call from the caller, disconnect it and call back to the caller. The limitation with this technique is that it requires extra hardware or software resources and increases call setup time[4].
Memory bound functions are implemented at the service provider and need the user to do some complex computation before the user is allowed to make the actual call. This complex computation will consume computing power at the senders’ device for every call he wants to make.[7] For spammers this means that they need much more hardware to make the same amount of calls, because of the computer power consuming computation. This will make it very expensive for a spammer to make a huge amount of spam calls in a short time; while the average user will not be bothered a spammer also has to pay for the extra calling costs that are made while the computation is solved.

– *HANDSHAKING/CHALLENGE/TURING TEST:*

Handshake/challenge/Turing tests are depending on the fact that some things are easy to do for humans, but almost impossible to do for a computer. This system is for example used in e-mail system, where the user has to recognize some letters from a picture with a lot of background noise [2]. A human user can easily distinguish the letters from the background noise, but a computer using optical character recognition will fail on this. However, there are systems know that are able to circumvent handshake/challenge/Turing tests in e-mail systems, as described in[5]. Handshake/challenge/Turing tests can also be adapted for the use in VoIP networks, where a user for example has to solve a little math question that is spoken out when he tries to call someone and pass back the correct answer. When the user provides the correct answer, he is instantly connected to the receiving user.

In contrast with Greylisting and memory bound functions with handshake/challenge/Turing tests the call will not lose it's instant character, because the test will cause almost no delay for a human user [2].

3) *STAGE 3: FEEDBACK FROM CALLEE AFTER CALLS*

The SPIT callers can be a human or machine. The callers are authenticated via their private-public key exchange or Turing test authentication process [6]. The complex puzzles has additional burden on callers which annoy them and also increases call setup time. The Payments at Risk based approaches verifies the nature of caller by first deducting money and then giving back if caller found to be legitimate. This solution requires either called feedback or analysis of speech content among users[9].

– *SIGNALLING PROTOCOL ANALYSIS*

VoIP calls consist of two parts: signalling and media data. Before every VoIP call signalling data for setting up a call is exchanged between the two end-users. Spammers are interested in the correct delivery of their calls, therefore the call routing information provided in the call setup request is valid and can therefore be used for further analysis. A second characteristic of spam calls is that they are unidirectional: the spammer initiates the calls to the targeted network, but nobody calls the spammer. A third characteristic is the termination behaviour, this is statistical consistent. This means that there is a pattern of which of the two calling parties terminates the call. A fourth distinction is, spammers do not call the same recipient for some period of time. Based on these characteristics of voice spam calls, it defines a number of scenarios for the statistical termination behaviour that can be distinguished. Based on a statistical analysis of this termination behaviour the authors claim that it is possible to achieve an accuracy of about 99.9%.

B. *INSTANTIATING THE PREVENTION MECHANISM*

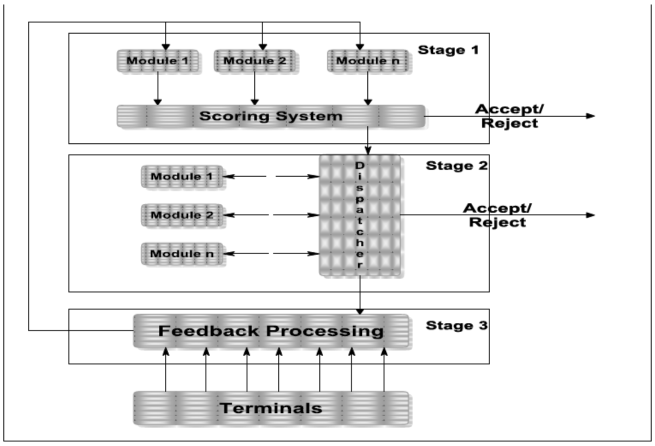

Fig 5 SPIT Prevention Mechanism

1) *SPIT Prevention at Stage 1*

Stage 1 design is based on a scoring system. Scoring system is similar to common email spam filters where the filtering methods detects whether email is a legitimate or spam.

Modules examine the incoming call signaling protocols and produce a score in a normalized range of [-1, 1]. The score indicates the likeliness of the call being SPIT with a highscore indicating high likeliness. The total score for each call is the weighted sum of all modules. Weights can be configured per module as well as the thresholds for the overall score. The total score is compared to two thresholds (a low and a high). If it is **below** the lower threshold, the call is forwarded to the callee. If it is **between** the lower and higher thresholds, the detection process is not complete, and the call is forwarded to the second stage modules for further processing. Otherwise, if the total score is **above** the higher threshold, either the call is rejected or forwarded to a voicemail system to not suppress the communication (which may be a legal requirement).

2) *SPIT Prevention at stage 2:*

At stage 2 modules containing prevention methods are called sequentially until a final decision on accepting or rejecting a call has been made. A configurable dispatcher calls the modules, processes their results, and makes the decision. For this method the dispatcher accepts the call on behalf of the callee and invokes the stage 2 module selected (e.g., a Turing test using voice communication). If the test is successfully passed, the dispatcher forwards the call to the original callee by referring the call, as shown in Fig. 5.2. Otherwise, the call is either immediately terminated or recorded.

3) *Greylisting:*

Greylisting is based on a simple rule that is applied to all incoming messages: each incoming message will be blocked unless the same IP address has tried to establish a call within the last N hours/minutes. When the sender is blocked, he will receive a message like "the user is currently busy". Normal users will then try to call back later. After the sender has called back his IP address is added to the whitelist and all future calls will be connected immediately. A great benefit of this system is the automatic maintenance, this causes very little work for both the administrator of the system and the user. When the used VoIP protocols are implemented correctly this techniques does not have any false positives, which is a great advantage, because this means that no calls will be blocked that should have reached the user.

A disadvantage of the system is that it is designed as a system complementary to existing systems and not to replace any systems, this means that you also need other protection techniques. For some users, especially some business users, the fact that the setup of a call will take longer, because the first attempt will be rejected will be a great disadvantage. But for most private users this will not be a great sacrifice if they know that spam will be eliminated. The technique is also not suitable for emergency calls or other urgent calls, because of the delay caused by the first rejection of the call.

V. COMBINATION OF THE TECHNIQUES

A. HANDSHAKE/CHALLENGE/TURING TESTS IN COMBINATION WITH GREYLISTING:

The combination of handshake/challenge/Turing tests with an automatically maintained greylisting will cancel out most of the disadvantage of user acceptance. When a caller passes the handshake he could be automatically added to the user's greylist, this will result in a system where the caller only has to meet the handshake once, instead of every time he calls. This scenario can be countered by adding an expiration time to the records on the greylist, because one of the characteristics of VoIP spam is that the same user will not be called by a spammer for an extended period of time. The expiration will remove the spammer from the user's greylist, so he has to meet the handshake again the next time he calls the user.[1]

B. MEMORY BOUND FUNCTION IN COMBINATION WITH GREYLISTING

The delay caused by memory bound functions can be partly cancelled out by combining memory bound functions with an automated greylist. When the caller has fulfilled his "proof of effort" he can be automatically added to the greylist of the user. This will result in a system where the caller has to only fulfil a "proof of effort" on his first call to the user; the next call will have no delay. As described in the previous section, once this system is known to spammers they could adapt their spam strategy accordingly.

This can be solved in the same way as described by adding an expiration time for the records on the user's whitelist. Another option to prevent this is to enlarge the time a caller must spend on his "proof of effort".

C. SIGNALLING PROTOCOL ANALYSIS IN COMBINATION WITH GREYLISTING

To lower the amount of false positives when signalling protocol analysis is used, this technique can be combined with greylisting. This will allow automated services as to be able to call the user, when the user has added this service to his greylist. According to the authors of, the addition of a greylist will provide a low false positive rate.[5]

VI. FUTURE WORK

The techniques that are available right now are perfectly good and are able to work with it but the main scenario can be opened when the combination of the various antispam techniques is done. Therefore the main target would be to combine above mentioned techniques and analyse and provide the result that which combination is the best one that we can use for further work. So there is not a single technique or combination of techniques that is most promising for the future, but there are several options. Practical information about the effectiveness of the identified suitable techniques and combinations of techniques needs to be researched to identify which of these techniques will be best to use in the future. The main combination that could be taken into account is with the greylisting technique because the combination of various anti-spam techniques with whitelisting have been performed theoretically purpose. So the main part can be a combined result of antispam technique with greylisting that can reduce or mitigate Spam Over Internet Telephony.

VII. CONCLUSION

There has been different various Antispam techniques as we have seen above in the paper. So the main possibility that we can have is to have various combination of the techniques that can be established to mitigate the spam calls in order to be effective. The combinations of techniques that are suitable for the future are: Handshake/challenge/Turing test in combination with greylisting, memory bound functions in combination with greylisting and signalling protocol analysis in combination with greylisting. VoIP spam protection will probably always stay an arms race between the spammers that are continuously trying to increase the more difficulties of the Antispam techniques and the researchers that develop new techniques or improve existing techniques for the particular problem to be solved but as shown with a combination of techniques most of the disadvantages can be cancelled out.

REFERENCES

[1] Vincent M. Quinten Analysis of spam over Internet telephony protection Techniques" 6th Twente Student Conference on IT, Enschede, 2nd February, 2007.

[2] Achraf Gazdar , Zeineb Langar, Abdelfettah Belghith "A Distributed Cooperative Detection Scheme for SPIT Attacks in SIP Based System", University of Manouba, Tunisia,2012 IEEE

[3] J. Rosenberg, C. Jennings, RFC 5039 - The Session Initiation Protocol (SIP) and Spam, IETF, 2008.

[4] Muhammad Ajmal Azad, Ricardo Morla "Mitigating SPIT with Social Strength" INESC TEC, Faculty of Engineering, University of Porto, Portugal, 2012 IEEE. Email {muhammad.ajmal, ricardo.morla}@fe.up.pt.

[5] Hemant Sengar, Xinyuan Wang,Art Nichols Technology Development Dept. Windstream Communication, Greenville,SC29601 \{hemant. senger, Arthur. nichols} @windstream.com"THWARTING SPAM OVER INTERNET TELEPHONY (SPIT) ATTACKS ON VOIP NETWORK", 2011 .

[6] Juergen Quittek, Saverio Niccolini, Sandra Tartarelli, and Roman Schlegel "On Spam over Internet Telephony (SPIT) Prevention," IEEE Communications Magazine • August 2008

[7] R. MacIntosh and D. Vinokurov." Detection and mitigation of spam in IP telephony networks using signaling protocol analysis". pp. 49-52, 2005.

[8] Alexander J. Johansen and Woraphon Lilakiatsakun " A VOIP ANTI-SPAM
SYSTEM BASED ON MODULAR MECHANISM DESIGN" Faculty of
Information Science and Technology, Mahanakorn University of Technology,
Bangkok, Thailand Emails: ajohansen@ieee.org, woraphon@mut.ac.th, NCIT 2010

[9] Muhammad Ajmal Azad, Ricardo Morla "Multistage SPIT Detection in Transit VoIP", Faculty of Engineering, University of Porto Portugal, muhammad.ajmal@fe.up.pt, ricardo.morla@fe.up.pt

[10] Chen Hongchang□Chen Fucai, Li Shaomei "A Multilayered Fusion Method for SPITs Detection" National Digital Switching System Engineering&Technological R&D Center,Zhengzhou 450002, cfc@mail.ndsc.com.cn , 2011 IEEE

[11] Stelios Dritsas and Dimitris Gritzalis "Information Security and Critical Infrastructure Protection", Research Group Dept. of Informatics, Athens University of Economics & Business (AUEB) 76 Patission Ave., Athens, GR-10434 Greece {sdritsas,dgrit}@aueb.gr "AN ONTOLOGY – DRIVEN ANTISPAM ARCHITECTURE".

[12] Lu Tian1, Nicolas Dailly, Qiao Qiao, Jihua Lu1, Jiannan Zhang, Jing Guo and Ji'ao Zhang"Study of SIP Protocol Through VoIP Solution of "Asterisk"" Beijing University of Posts and Telecommunication, Dept of Computer and Telecom Networks.

[13] Evan Harris. The Next Step in the Spam Control War: Greylisting. http://projects.puremagic.com/greylisting/whitepaper. html, (24-09-2006), Evan Harris, 2003.

[14] Hu Yin, Zhang Chaoyang "An improved Bayesian Algorithm for Filtering Spam E-mail" 2011 International Symposium on Intelligence Information Processing and Trusted Computing

[15] Gonzalo Garateguy, Gonzalo R. Arce, Juan Pelaez "Covert Channel detection in VoIP streams" 2011 IEEE