Journal of Engineering Technology Vol. 6: 55-59, 2018
ISSN 2231-8798

Alerting SPAM over Internet Telephony (SPIT) Network Threats

Ahmad Roshidi Amran[1], Mohamad Ikmal Abdul Rahman[1], Mohd Raziff Abdul Razak[1] & Amna Saad[2]
[1]Telecommunications Technology Section
Universiti Kuala Lumpur British Malaysian Institute, Gombak Selangor.
[2]System & Networking Section
Universiti Kuala Lumpur Malaysian Institute of Information Technology, Kuala Lumpur.
Corresponding email: aroshidi@unikl.edu.my

Abstract: VoIP system use an Internet Protocol (IP) network; VoIP are prone to network attacks by third party through a lot of ways and one of them is through spamming. Spam can be defined as an unsolicited bulk message sent from one internet user to the other purposely used to mainly cause Denial of Service in a VoIP system, it is called Spam over Internet Telephony (SPIT). This research paper focusing on producing a test environment utilizing open source platforms that include Intrusion Detection System (IDS) with performance analysis. Kali Linux 2.0 will be used to illustrate the attack while Snort which is IDS software will work as a database that will monitor packet entering and leaving the system. The system developed successfully alerting end users or network administrators for any suspicious Session Initiation Protocol (SIP) that could contribute to the spreading of SPIT.

Keywords: SPIT, IDS, Kali Linux, VoIP, Snort, Spam

1.0 INTRODUCTION

Voice over Internet Protocol (VoIP) is one of the methods to interact in voice conferencing that is much more suitable voice services in Internet Protocol (IP) network environment as compared to standard telephony Public Switch Telephone Network (PSTN). One of the advantages of VoIP compared to a standard telephony is the lower cost to interact with other end users. The reason is that VoIP only require internet connection to communicate that has become a must in each house in this 21st century.

However, due to this system depending very much on IP network, it becomes vulnerable to network attacks especially spam. Spam is an unsolicited bulk message sent from one internet user to other internet user that is used to obtain information without permission. Since this spam problems occur in VoIP system, it is called Spam over Internet Telephony (SPIT). However, SPIT is much more nuisance compared to spam in an email since end users need to manually pick up the phone receiver even during midnight but only to realize that it is just a spam.

The spam may come in the form of messages, telemarketing or even advertising. This nuisance can disrupt the end user activity. If the phone gets infected, it will then spread the spam to the other end users via the infected user contact list. This can cause a massive unpreventable problem. As stated by Malaysian Computer Emergency Response Team (MyCERT), first quarter of 2011 which is from January to March as shown in Figure 1 below; 80 per cent of the spam distributed in Malaysia is coming from Asia and bear in mind that 70 per cent from that 80 per cent was coming from Malaysia itself [1].

This became evident that it takes only three months to generate a huge amount of spam distributed into Malaysia that could disrupt every Malaysian daily activity.

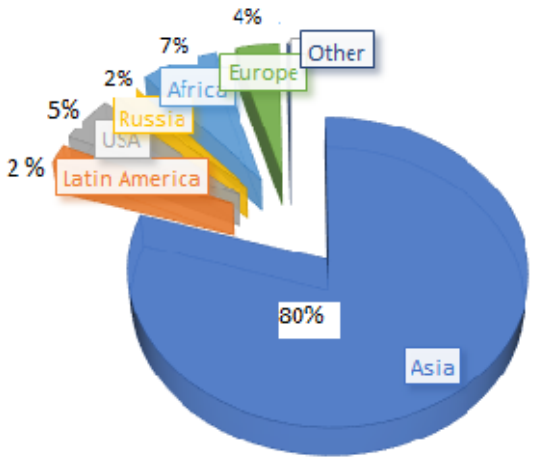

Figure 1. Sources of Spam distribution in Malaysia based on regions [1]

Journal of Engineering Technology Vol. 6: 55-59, 2018
ISSN 2231-8798

As such, research into developing an alert SPIT system that successfully detect any suspicious SIP could pave the way to creating a solution to mitigate this problem will become vital in the future. We focused in developing the system focusing with performance analysis during occurrence of an attack.

First and foremost, research done by Ram Dantu and Prakash Kolan concentrating on creating a solution to provide security for VoIP system on real-time compared to standard spam which is email spam using social meaning of trust and reputation [2]. They used closed loop feedback between different stages in deciding whether the call is a spam call or not alongside measuring the accuracy of the filter as illustrated in Figure 2. A lot of stages proposed by the authors such as Presence, Rate Limiting, Black and White Listing and Bayesian Learning. However, due to the amount of stages needed to be done to determine the call is spam or not, it will result in delays in the SIP set up time. This is good if the caller is spam but if the caller is a genuine caller then this proposed solution could cause a slight inconvenience in terms of Quality of Service for voice (QoS) for the genuine caller.

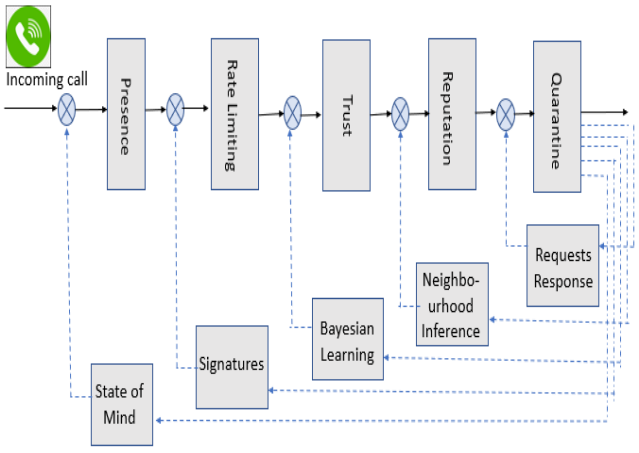

Figure 2. Loop feedback functional elements.

In a different approach by Janne Lindqvist and Miika Komu they concentrate to mitigate SPIT using Human Interactive Proof (HIP) and focusing on Session Initiation Protocol (SIP) [3]. HIP work similar to the meaning of trust and reputation proposed by Ram Dantu and Prakash Kolan which they provide some ways to determine the call is genuine call or some automated call or spam call. They insert some implementation possibilities for VoIP system security such as End-to-end Approach, Proxy-Based Approach, Standardize Approach and Ad-Hoc Approach. However, the authors commenting that the proposed solution cannot work as a single solution and need to be combined to provide the best reliable security for VoIP system.

Besides that, these combinations of solution to produce the best methods for the VoIP system were also written by other authors such as Saeed Farooq Khan, Marius Portmann and Neil W. Bergmann on A Review of Methods for Preventing Spam in IP Telephony [4] alongside Vincent M. Quinten on Analysis of Spam over Internet Telephony Protection Techniques [5] and Remco van de Meent, Aiko Pras and Vincent M. Quintin on Analysis of Techniques for Protection Against SPIT [6]. However, these authors once again clearly stating that these techniques need to be combined to produce other technique that much more reliable that could neglect the weakness for example the combination of Signaling Protocol Analysis with Whitelisting. This will result in a lot of process need to be done before the call is being determined whether it is a spam call or not and inconvenient if the call is a genuine call.

Research done by Ruishan Zhang and Andrei Gurtov concentrating on a single technique which is collaborative reputation-based voice spam filtering [7]. They stated that this technique using call duration to derive his/her reputation value and leverage user feedback to mark unsolicited calls. Architecture for this Collaborative Reputation-based technique is illustrated in Figure 3. However, this technique somehow was not user friendly since the first call made by a genuine caller will also be provided with duration and he/her need to call back for the second time to assign the reputation value to them as a genuine call. Lastly, alerting SPAM using Intrusion Protection System (IPS) has also been conducted by the main author and fellow researchers [8]. The drawback is IPS would require a large amount of system resources to perform well.

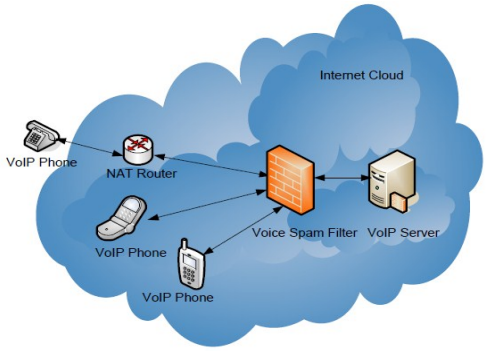

Figure 3. Collaborative-based technique network architecture

2.0 MATERIALS AND METHODS

A LAN network containing genuine IP phones, cisco router, switch, VoIP Asterisk server, attacking computer and laptop were set up as shown in Figure 4. A single network with network address 192.168.0.0/24 was configured as a main network. The network would the target network prone to SPIT attack where the victims would be users of VoIP phone in that network.

Journal of Engineering Technology Vol. 6: 55-59, 2018
ISSN 2231-8798

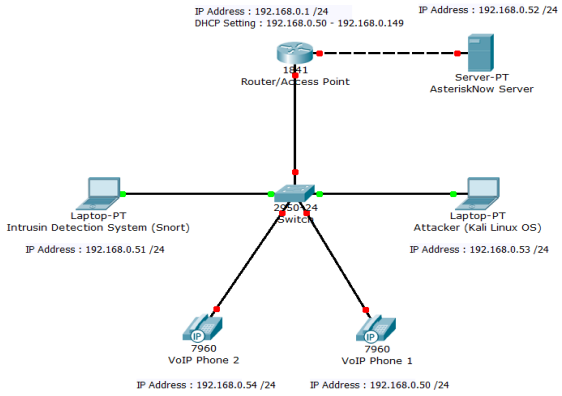

Figure 4. Network design and topology for the testbed

We used three main software which are Kali Linux 2.0, Snort and PRTG Network Monitor. First, Kali Linux 2.0 was as an attacking tool to launch an attack from a rogue user on genuine IP phone user. The software is an open source that run as Linux Operating System (Kali distro) under Debian distribution. It was designed for digital forensics and penetrations testing that was funded by Offensive Security Ltd and developed by three core developers which are Mati Aharoni, Devon Kearns and Raphael Hertzog [9]. They have invented the motto "The quieter you become, the more you are able to hear". This attacking tool is preinstalled with over 600 penetration-testing programs including Wireshark and Armitage. Its main interface is depicted in Figure 5.

Figure 5. Kali Linux 2.0 interface

Snort is also an open source and was used as an IDS that can sniff packets performing the real-time traffic analysis, packet logging, protocol analysis and content searching and matching. The computer that run snort was configured to run in intrusion detection mode that will monitor network traffic and analyses them based on a set of rules contributed by developers and contributors of Snort. Snort works by filtering any traffic in the network that match the criteria mention in the rules that configured by the admin user. Figure 6 shows a snapshot of a Snort configuration using command prompt.

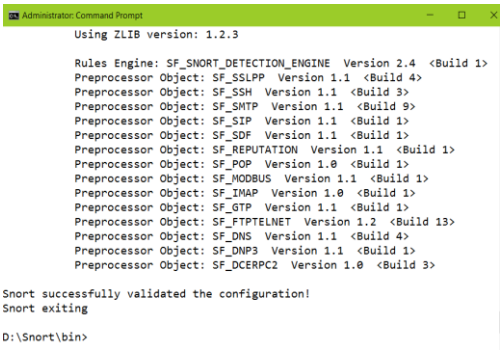

Figure 6. Snort configuration using command prompt

Finally, network performance will be thoroughly analyzed based on the bandwidth performance of the network during the attack using Paessler Router Traffic Grapher (PRTG) Network Monitor. It is intuitive network monitoring software developed by Paessler AG and contain hundreds of sensors preinstalled such as Simple Network Management Protocol (SNMP), Packet Sniffer and Netflow [10]. Figure 7 illustrates PRTG Network Monitor interface.

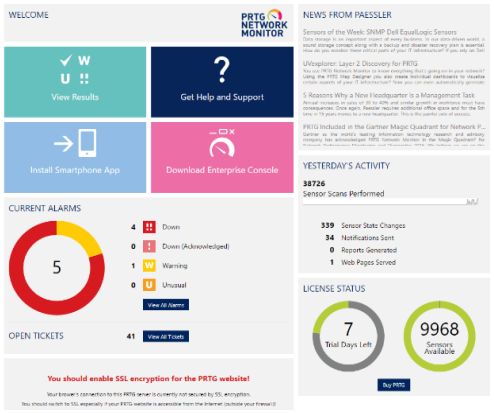

Figure 7: PRTG Network Monitor interface

3.0 RESULTS AND DISCUSSION

The attack launched using Kali Linux 2.0 was successful using the specific sub-software called metasploit. The attack would be broadcasted to the whole 192.168.0.0 /24 network. So, every IP phone user inside that network would be attacked and this is illustrated in Figure 8 below using Linux terminal. SPIT attacked was executed by flooding faked SIP packets on the network.

Journal of Engineering Technology Vol. 6: 55-59, 2018
ISSN 2231-8798

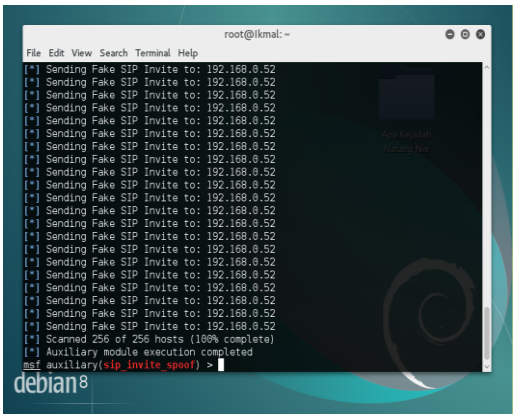

Figure 8. Successful attack to 192.168.0.0 /24 network

After the attack, Snort would alert for any detected malicious packets that travel inside 192.168.0.0 /24 network. However, for Snort to work, a set of rules is assigned beforehand as a reference for Snort. These are part of snort preprocessor where the rule set searches among others, the pattern "Invite" in the header fields of a SIP message alert, udp any 5060 -> any any (the first any is a source IP address followed by a udp port number and the second any is a destination IP address after the arrow which denotes flow with a running udp port number as represented by the third any) . SIP traffic commonly used port 5060 to initiate session in VoIP. The monitoring session and logging session done by Snort and these are depicted in Figure 9 and Figure 10 respectively. Snort has alerted on the suspicious/ malicious packets and logged them into Snort logging system for future reference.

```
05/08-03:21:59.263692  [**] [1:3000001:0] SIP [**] [Priority: 0] {ICMP} 192.168.0.53 -> 192.168.0.50
05/08-03:21:59.263692 192.168.0.53 -> 192.168.0.50
ICMP TTL:64 TOS:0xC0 ID:27149 IpLen:20 DgmLen:576
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.50:5060 -> 192.168.0.53:52829
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:742 DF
Len: 714  Csum: 61145
(520 more bytes of original packet)
** END OF DUMP
```

Figure 9. Alerting user on suspicious SPIT packet

```
To: <sip:192.168.0.52>
Via: SIP/2.0/UDP 192.168.0.50
From: "The Metasploit has you"<sip:192.168.0.53>
Call-ID: 100192.168.0.50
CSeq: 1 INVITE
Max-Forwards: 20
Contact: <sip:192.168.0.52>
```

Figure 10. Suspicious packet logged into the system

Due to the broadcast nature of the attack, it disrupted the bandwidth severely. This is evident that SPIT is dangerous type of spam that could cause a network to be congested and thus, bandwidth wastage. The bandwidth performance graph using PRTG Network Monitor is shown in Figure 11. A bursty transfer rate for SIP traffic was detected during the SPIT attack.

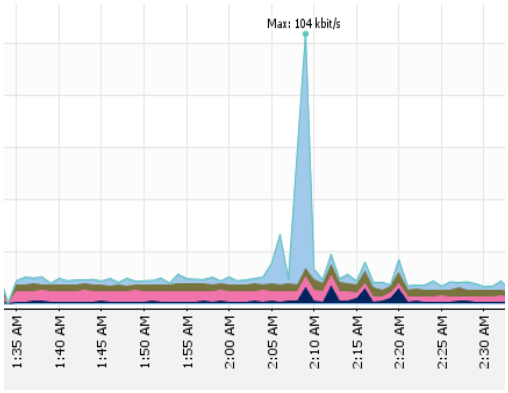

Figure 11. Network performance severely affected by the attack

The attack was launched by Kali Linux through Metasploit built into Kali Linux. The attacked was broadcasted to the whole network and monitored by Snort. Snort alerted user and logged the packet into logging system for network monitoring purposes. However, Snort will differentiate a standard packet that pass through the network with the packet that match the criteria mentioned in rules set. Snort will pass all packets to VoIP Asterisk server when no malicious packets are detected. Otherwise; It will produce alerts and log them. This can be summarized in the flow diagram in Figure 12 below.

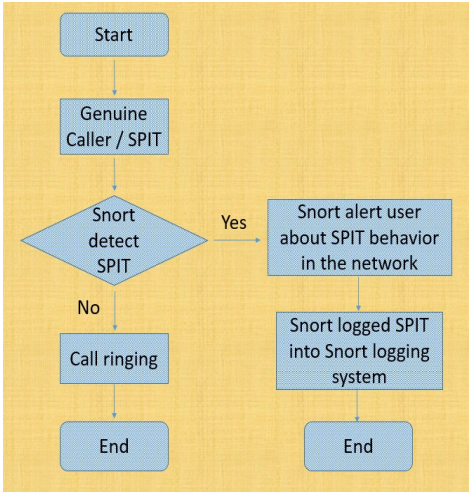

Figure 12. Alerting SPIT flow diagram

As mentioned before, the network performance is severely affected during the attack. It disrupted the bandwidth performance and would affect any user who used that network by congesting the network and flooding

the network with SIP fake packets. When the network is congested, any session done in that network will take a longer time to complete and thus, affecting other genuine IP phone user(s) in which, even the session cannot be completed at all.

This VoIP system use Internet Protocol (IP). As such the system is prone to network attacks by third party through a lot of ways and one of them is through spamming. Spam can be defined as an unsolicited bulk message sent from one internet user to the other purposely used to get confidential information without owner`s permission and since it occurs in VoIP system, it is called Spam over Internet Telephony (SPIT). This paper has demonstrated the attack simulated using Intrusion Detection System (IDS) such as snort and the attack is evident as demonstrated in the previous section, with some performance analysis. Kali Linux 2.0 was used as an attacking tool and the evidence is captured using snort, acting both as an IDS and a syslog server that monitor packets entering and leaving the system. The system successfully alerting end users or network administrators for any suspicious Session Initiation Protocol (SIPs) contributing to the spreading of SPIT.

5.0 CONCLUSION

In conclusion, this research will help VoIP admin user in the future in terms of providing a reliable security from any Spam over Internet Telephony. This is due to the growing demands for VoIP services. Even though several works had been done to create a reliable security for VoIP system such as the work proposed by Vincent M. Quinten which are whitelisting, blacklisting, grey listing etc. This research paper focusses on a single solution which is to mitigate and prevent SPIT using IDS software called Snort but on multiple network devices and security appliances. This research paper has met the objective to develop a solution to provide an alert system for SPIT and analyze the performance of the network during the attack. It also proven vital to come out with a solution to prevent SPIT from spreading inside a network that could result in congestion. Finally, the system developed can be used for further research by other prospective researchers.

A further recommendation will be stated in this subsection that any suspicious SPIT packets could be blocked entirely by using Intrusion Prevention System. This recommendation could prove more vital since it will eliminate the whole SPIT before it reaches end users and thus, indirectly eliminate the nuisance that come from SPIT. Nevertheless, this would be costly taking into considerations how expensive these software are. On the other hand, a more adequate software for network monitoring could be used in the future to replace existence network monitoring used in this project such as using Wireshark that proven more adequate. Moreover, a Linux could be replaced by a Windows operating system for further recommendation since a lot of software tools were originally made for Linux OS. It could prove to be more helpful and widespread to simulate and develop the Alert system using open source rather than using Windows that need a lot of others commercial software just to run a single tool which can be very costly.

REFERENCES

[1]. Sahrom Md Abu, Sharifah Roziah Mohd Kassim. “SPAM, the Annoying Culprit on the Net”. Cyber Security Malaysia. Vol 28 Q3 2011.

[2]. Ram Dantu, Prakash Kolan. “Detecting Spam in VoIP Networks”. SRUTI 2005: Steps to Reducing Unwanted Traffic on the Internet Workshop. Dept. of Computer Science and Engineering, University of North Texas. 2005.

[3]. Janne Lindqvist, Miika Komu. “Cure for Spam over Internet Telephony”. Helsinki Institute for Information Technology. 2007.

[4]. Saeed Farooq Khan, Marius Portmann, Neil W. Bergmann. “A Review of Methods for Preventing Spam in IP Telephony”. School of Information Technology and Electrical Engineering, University of Queensland, Australia. 2013.

[5]. Vincent M. Quinten. “Analysis of Spam over Internet Telephony protection techniques”. 6th Twente Student Conference on IT. University of Twente. 2007.

[6]. Vincent M. Quinten, Remco van de Meent, Aiko Pras. “Analysis of Techniques for Protection against Spam over Internet Telephony”. University of Twente. 2007.

[7]. Ruishan Zhang, Andrei Gurtov. “Collaborative Reputation-based Voice Spam Filtering”. Helsinki Institute for Information Technology. 2011.

[8]. Amna Saad, A. Roshidi Amran, Izzat Norhalim, M. Adib M. Yusof. “Automated Intrusion Detection and Prevention System over SPIT (AIDPoS). 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET). University Kuala Lumpur. 83 – 88. 2015.

[9] Kali Linux 2.0 brief explanation retrieved from: www.kali.org/about-us

[10] Paessler AG, https://www.paessler.com/prtg; Last retrieved December 2017