Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Pruthvika Kadu, IJPRET, 2014; Volume 2 (9): 1018-1024 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

AN OVERVIEW ON IPV6 AND SPAM

PRUTHVIKA S. KADU[1], DR. H. R. DESHMUKH[2], PROF P.G. ANGAITKAR[3], S. A. KARALE[3]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Prof and HOD, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
3. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Spam has posed a serious problem for users of email since its infancy. Today, automated strategies are required to deal with the massive amount of spam traffic. IPv4 networks offer a variety of solutions to reduce spam, but IPv6 networks' large address space and use of temporary addresses both of which are particularly vulnerable to spam attacks makes dealing with spam and the use of automated approaches much more difficult. IPv6 thus poses a unique security issue for ISPs because it's more difficult for them to differentiate between good IP addresses and those that are known to originate spam messages.

Keywords: IPv6, Spam, Antispam technologies

PAPER-QR CODE

Corresponding Author: MS. PRUTHVIKA S. KADU

Access Online On:

www.ijpret.com

How to Cite This Article:

Pruthvika Kadu, IJPRET, 2014; Volume 2 (9): 1018-1024

INTRODUCTION

The prevailing Internet Protocol standard is IPv4 (Internet Protocol version 4), which dates back to the 1970s. There are well-known limitations of IPv4, including the limited IP address space and lack of security. IPv4 specifies a 32-bit IP address field, and available address spaces are rapidly running out. The only security feature provided in IPv4 is a security option field that provides a way for hosts to send security and handling restrictions parameters[1].

As a result, the Internet Engineering Task Force (IETF) has been working on the IPv6 (Internet Protocol version 6) specifications in order to address these limitations, along with a number of performance, ease-of-configuration, and network management issues. The core IPv6 specifications have been defined by various Request for Comments (RFCs) such as RFC 2460[2] (IPv6 Protocol), RFC 4861[3] (IPv6 Neighbour Discovery), RFC 4862[4] (IPv6 Stateless Address Auto-Configuration), RFC 4443[5] (Internet Control Message Protocol for IPv6 (ICMPv6)), RFC 4291[6] (IPv6 Addressing Architecture), and RFC 4301[7] (Security Architecture for IP or IPsec). IPv6 is also referred as the Next Generation .

LITERATURE REVIEW

Why IPv6 Is Important

In IPv4 networks, the largest daily amount of traffic after file sharing is traffic related to SMTP usage; unfortunately, a large percentage of that SMTP traffic is spam. According to the spam cop blacklist report, spammers generate approximately 7.5 messages per second each month According to Google statistics the use of IPv6 has increased dramatically since 2010, as has the use of SMTP, which is a main protocol running within IPv6 networks. According to AMS-IX (a mainline router), the average daily traffic of IPv6 is 2.7 Gbytes, which is roughly 4 percent of the Internet's total traffic. This means that more ISPs are supporting IPv6 and thus there's more IPv6-related traffic.

Spam in IPv6 Networks

The IPv6 network supports 2^128–32 times more unique IP addresses than IPv4. Generally, service providers allocate prefix ranges to each home or small business network. Each of these networks would therefore have direct control over at least 2^64 unique IP addresses within their assigned subnet. Spammers might search for insecure SMTP-enabled computers in these networks. They might then start sending spam messages using different IP addresses accessible in that subnet. The sheer size of the addressable IPv6 address space threatens to render useless many antispam technologies that are based on IPv4 addresses, such as IP blacklisting.

What Spam Can Do

Spammers use forged messages, stolen identities, bogus cancellation addresses, and relay hijacking to hide their identities when sending their advertisements or bogus messages. This activity uses a lot of Internet bandwidth. We can categorize spam issues from both the client and server perspectives. From the client perspective, if users receive more than 40 spams per day and need an average of 10 seconds each to decide what to do with them, they'll be wasting approximately 60 hours a year — more than seven work days — dealing with spam. Moreover, if users have limited Internet access on their mobile phones, they might have to pay extra each month just for downloading spam messages. Users clearly waste both money and time downloading spam. From a server perspective, processing numerous messages thrust onto the server, especially at the same time, can lead to a system crash or prevent users from sending or receiving messages (DoS attack).

Spammers also search open mail relays, SMTP servers that let anonymous Internet users send mail to deceive people with fraudulent messages. They can deceive inexperienced Internet users by using spammers' bluffs — that is, by misrepresenting themselves and their business enterprises. They can also send messages to a list of mail addresses obtained using software that crawls through Internet web pages.

Although outside our article's scope, the general definition of spam that we gave earlier can also be applied to the use of malicious programs, malware, or worms called bots that are attached to messages sent to people to infect other computers on the Internet. These infected computers, or zombies, give spammers full access to the computers' resources, letting them control the computers and either launch DoS and phishing attacks[8] on websites or disseminate additional malware.

As an example, consider a scenario in which attackers wish to misuse the DNS round-robin technique, which is used to balance the load among servers. To do this, attackers use a "fast-flux" technique to change an IP address and infect the client's computer and then use that computer's resources for further attacks When a host resolves a domain name, the DNS server replies with a large list of IP addresses corresponding to that domain. According to the round-robin technique, the client DNS chooses one of these addresses (the attackers' computer) to gain access to one of the bots. The bot then acts like a proxy to direct a host to a malicious website the attacker controls[9].

Categorizing Spam

The general term "spam" is commonly used to refer to any unwanted unsolicited

electronic message. In this report, we focus on email-related spam, but other types, such as instant-messaging (IM) spam or Internet-telephony spam, are also of concern. This section describes the properties of the various types of spam.

- **Email Spam**

Spam for purposes of discussion here, is considered unwanted, unsolicited bulk email (UBE) or unsolicited commercial email (UCE). The main objective of UBE and UCE is to provide direct advertising to the largest possible audience at the lowest possible cost. New technologies such as email lower the costs of distributing advertising and have enabled the growth of spam. There are many costs associated with email spam, including the costs of lost productivity, user education, network-infrastructure loads, and development and deployment of antispam technologies. The common properties that help identify a message as spam are that: the source of the message cannot be trusted or authenticated; the costs incurred by the sender are often less than the total costs incurred by the recipients; and the content of the message contains unwanted offensive, fraudulent or deceptive material. For spam email to be delivered, a list of target email addresses has to be compiled. A common way to acquire valid email addresses is through "harvesting." Harvesting is done using automated software that can scour public databases and websites for email addresses. Once a list of recipients is obtained, software tools can be used to formulate the content and header of each message. These headers and contents are customized to hide the source and bypass anti-spam technologies such as filters. The messages can then be sent using automated tools to distribute the transmission load across various sources (relays, proxies, etc.).

A user should be aware of how spammers get addresses, as well as how they collect data about their message recipients. For instance, some spam email may provide an

unsubscribe option at the end of the email. A user should be cautious in using this option, however, since it can be used for malicious purposes. The link can let a spammer identify which recipients have read the message. This can, consequently, increase the amount of spam a user receives. The unsubscribe option may also link to content that contains a method for exploiting vulnerabilities in the recipient's web-browser software. In some cases, these "exploits" are used to install malicious software on the recipient's computer, which can then be used to transmit spam to others.

- **Spam for Instant Messaging**

Instant messaging (IM) can also be used as a medium for sending spam — hence the

name spam for instant messaging (SPIM). Internet-based IM services, like MSN Messenger, Yahoo! Messenger and Jabber, can also be used to transmit spam. In the case of Internet-based IM services, a directory is often used to locate and identify subscribers. The directory services can be used to harvest usernames and, subsequently, send individual messages to each subscriber. This process can be automated using software; however, the sender must also be a user of the IM system. Most IM systems now block, by default, messages from unknown senders, and provide users with the ability to block specific senders.

- **Spam Over Internet Telephony**

Voice over Internet protocol (VoIP) has the potential to lower the cost to advertisers of

sending direct voice communications to a target audience. The transmission of spam using VoIP, also dubbed spam over Internet telephony (SPIT) involves using an Internet

connection to place calls or leave messages to VoIP subscribers. The costs associated with VoIP spam are higher than for email spam or SPIM, since senders of audio messages incur higher costs for the bandwidth used. The method for sending SPIT is similar to that for sending other spam; automated software can be used to

establish connections to a VoIP terminal. Once a connection is made, a message can be sent as audio or recorded as voicemail. Unlike telemarketing, VoIP spam can be sent over Internet connections, where trust and traceability are often lacking. The use of secure network architectures can protect subscribers from receiving calls from untrusted callers. However, non-technical methods may be needed to mitigate spam for VoIP services.

Anti-Spam Technologies

There are many solutions that can be used to combat the various types of email-based

spam. Filtering messages based on their properties, blocking message senders, ensuring senders are authentic, and authorizing clients are all methods used to combat spam.

1) Message Filtering

In general, implementing message filtering is straightforward and does not require any

modifications to existing email protocols. A good filter design will minimize the number of false positives (filtering of a message that is not spam) and maximize the efficiency of the filter. Filters simply prevent spam from entering inboxes, but do not stop the generation of spam. This section gives an overview of the common types of filters, including hybrid filters that use combinations of filtering methods.

2) Content Filters

There are many varieties of content filters, but, as the name suggests, they all simply filter based on the content of the message. The filter rules are normally defined for all

local users on an MTA by a system administrator. Rules can be set for any content in the header, body or extensions of a message. The filter can be configured to analyze or parset he header for malformed fields, to parse the body of the message for spam-related content, or to examine message extensions such as attachments.

Most content filters also have a high rate of false positives, especially when legitimate

mail contains content similar to that in the filter's rule set. The content filter rules must be constantly updated to stay effective. Spammers adjust their messages to bypass filters, and these bypass methods have led to oddly worded content and image-only spam.

3) Hashing Filters

Once enough spam has been observed, common elements can be collected. These common elements can be "hashed" to give a unique value that, in turn, is stored and used as a filter rule. When a hashing filter processes a message, the common elements are collected and hashed. The unique value is then used to determine if the common elements were previously categorized as spam; if so, the message can be filtered as spam. The filters can be bypassed, however, by inserting insignificant content into the message to disrupt the processing of common message elements.

4) Statistical Filters

As an improvement to content and hashing filters, statistical filters use rules to measure

the frequency and patterns of email messages. The most popular statistical filter used for spam is the Bayesian filter. Bayesian filters calculate the likelihood of known elements combining with additional elements in order to obtain an overall likelihood ratio that can be used to categorize a message as being legitimate or spam[10].

CONCLUSION

It's clear that in IPv6, network spammers have one ext ra, power ful weapon at their disposal — the large address space — so DNS based, blacklisting, and gray listing solutions can't continue working as before without prefix blacklisting. IPv6 has several security features such S IP sec, which authenticates and encrypts each IP packet used during communications.

REFERENCES

1. http://www.ietf.org/rfc/rfc0791.txt

2. http://tools.ietf.org/html/rfc2460

3. http://tools.ietf.org/html/rfc4861

4. http://tools.ietf.org/html/rfc4862

5. http://tools.ietf.org/html/rfc4443

6. http://tools.ietf.org/html/rfc4291

7. http://tools.ietf.org/html/rfc4301

8. S. Suwa et al., "DNS Resource Record Analysis of URLs in Email Messages for Improving Spam Filtering," Proc. IEEE/IPSJ Int'l Symp. Applications and the Internet, 2011, IEEE CS Press, pp. 439–444.

9. F. Paget, "From Fast-Flux to RockPhish," McAfee Blog Central, 30 Nov. 2007; http://blogs.mcafee.com/ mcafee-labs/from-fast-flux-to-rockphish-part-1.

10. Anti-Spam Technical Alliance, Anti-Spam Technical Alliance Technology and Policy Proposal, June 2004 (http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf)