IGI PUBLISHING **ITJ4224**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 2, Issue 2
edited by **Hamid R. Nemati © 2008, IGI Global**

Spam Classification Based on E-Mail Path Analysis

Srikanth Palla, University of North Texas, USA

Ram Dantu, University of North Texas, USA

João W. Cangussu, University of Texas at Dallas, USA

ABSTRACT

Email spam is the most effective form of online advertising. Unlike telephone marketing, email spamming does not require huge human or financial resources investment. Most existing spam filtering techniques concentrate on the emails' content. However, most spammers obfuscate their emails' content to circumvent content-based spam filters. An integrated solution for restricting spam emails is needed as content analyses alone might not provide a solution for filtering unsolicited emails. Here we present a new method for isolating unsolicited emails. Though spammers obfuscate their emails' content, they do not have access to all the fields in the email header. Our classification method is based on the path an email traverses instead of content. Overall, our classifier produced fewer false positives when compared to current filters such as SpamAssassin. We achieved a precision of 98.65% which compares well with the precisions achieved by SPF, DNSRBL blacklists.

Keywords: *spam detection, path analysis, relay analysis*

INTRODUCTION

E-mail spam is the electronic equivalent of "postage-due" junk mail. Spamming involves sending nearly identical unsolicited messages to thousands or millions of recipients. Out of all the problems pestering the present day e-mail infrastructure, spam has evolved into a nettlesome problem. Unlike its conventional cousins (postal mail and telemarketing) e-mail spam imposes its transactional costs directly on the recipient. Spam can be sent anonymously and turns out to be a highly profitable marketing technique despite some costs incurred in procuring e-mail addresses and dispatching the spam e-mails.

Spam causes more economic damage than hackers or any malware. A London-based computer security firm mi2G (Lemke, 2003) reported that computer outages and lost productivity because of spam led to $10.4 billion in worldwide economic losses whereas viruses and worms cause $8.4 billion in losses, while hackers contribute to $1 billion in financial damage worldwide. Though a wide variety of

spam filters and other techniques are currently in use they have not been successful in restricting spam and fraudulent e-mails completely from reaching the recipient.

In recent years there has been a great influx of various spam filtering approaches such as rule-based spam filtering techniques (William, 1996), statistical filtering approaches (Massey, Mick, Raya, & Scott, 2003), machine learning, Bayesian classifiers (Graham, 2003), combinations of rule based and Bayesian approaches (Spa, 2006), and spam filtering using contextual network graphs (Kelleher, 2004). In spite of all these techniques, spam remains an annoying problem because a majority of the spam filtering techniques focus on the content of an e-mail, which is in complete control of the spammers. However, most of the spammers obfuscate their e-mail content in order to circumvent these spam filters. Lowed and Meek (2005) report that a spammer can get through 50% of the blocked spam past the filters by adding 150 or fewer words. If a spammer is able to send test messages to the targeted spam filter, 30 words is sufficient in getting half of the blocked spam through the filters.

Here a new classification method based on the path traversed by an e-mail is proposed. Spammers can forge certain fields in the e-mail header but cannot modify the complete path traversed by an e-mail. Using this information the proposed approach has been able to accurately identify e-mails as legitimate or spam. To achieve this level of accuracy, reputation and trustworthiness of the relays and path traversed by an e-mail are also taken into account. This approach improves upon content analysis as spammers frequently obfuscate their e-mails content. In addition, a social network analysis is also conducted. In this analysis the classifier is fine tuned according to the recipient's social network resulting in a considerable reduction of false positives and false negatives generated by the classifier.

The remainder of this article is organized as follow. An overview of several spam filtering techniques including whitelists, blacklists, greylists, machine learning, e-mail authentication, and social networks is presented in Section II. The proposed methodology for the spam identification is delineated in Section III. Section IV presents the validation of the approach using two e-mail corpuses. Also presented in Section IV is a qualitative as well as a quantitative comparison of the proposed approach with relevant existing work. Finally, conclusions as well as potential improvements of the proposed classifier are presented in Section V.

RELATED WORK

A wide variety of filtering techniques and other methods are currently used to restrict spam and phishing e-mails from reaching the user's inbox. Client- and server-side spam filtering using blacklists, whitelists (Hird, 2002) and greylists (Levine, 2005), text classification methods based on predefined rules, Bayesian filtering, pattern recognition, and identity recognition are a few filtering mechanisms currently being used. Also available are e-mail authentication standards such as identified Internet mail (IIM), domain keys identified Internet mail (DKIM), sender policy frame work (SPF), sender ID frame work, and so forth, which identify genuine senders from spammers and fraudsters. In addition to these approaches, new methods based on senders' reputation and accreditation services are emerging rapidly. Next, various spam filtering techniques are briefly discussed. To the best of our knowledge no existing technique applies a multivariate analysis comprising the four analyses described later in Section III.

Spam Filtering using Whitelists, Blacklists and Greylists

Normally client and server side spam filtering is achieved through maintaining a list of trusted and untrusted senders. The list of trusted senders is termed whitelist (Hird, 2002) and the list of untrusted senders is known as blacklist (Hird, 2002). E-mails from the whitelisted senders are not subjected to any filtering mechanisms and delivered to the recipient. The recipient might have sent or replied to the e-mails of the whitelisted senders in the past. The address book of the recipient is normally used as a whitelist.