Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Caller-REP: Detecting unwanted calls with caller social strength

*Muhammad Ajmal Azad**, *Ricardo Morla*

Faculty of Engineering and INESCTEC, University of Porto, Porto, Portugal

ARTICLE INFO

Article history:
Received 26 December 2012
Received in revised form
15 July 2013
Accepted 23 July 2013

Keywords:
SPIT
VoIP
Reputation
Social network analysis
Trust

ABSTRACT

Voice over IP (VoIP) is a cost effective mechanism for telemarketers and criminals to generate bulk spam calls. A challenge in managing a VoIP network is to detect spam calls without user involvement or content analysis. In this paper we present a novel content independent, non-intrusive approach based on caller trust and reputation to block spam callers in a VoIP network. Our approach uses call duration, interaction rate, and caller out-degree distribution to establish a trust network between VoIP users and computes the global reputation of a caller across the network. Our approach uses historical information for automatically determining a global reputation threshold below which a caller is declared as socially non-connected and as a spammer. No VoIP data-set is available for testing the detection mechanism. We verify the accuracy of our approach with synthetic data that we generate by randomly varying the call duration, call rate, and out-degree distributions of spammers and legitimate users. This evaluation shows that our approach can automatically detect spam callers in a network. Our approach achieves a false positive rate of less than 10% and true positive rate of almost 80% in the first two days even in the presence of a significant number of spammers. This increases to a true positive rate of 99% and drops a false positive rate to less than 2% on the third day. In a network with no spammers, our approach achieves a false positive rate of less than 10%. In a network heavily saturated with more than 60% of spam callers, our approach achieves a true positive rate of 98% and no false positives. We compare the performance of our approach with a closely related spam detection approach named Call-Rank. The results show that our approach outperforms Call-Rank in terms of detection accuracy and detection time.

1. Introduction

VoIP is generally used to provide cheap telephony service in Internet Protocol (IP)-based networks. The use of IP for the transmission of voice leaves VoIP vulnerable to denial of service and service abuse attacks from the malicious users (Keromytis, 2011). One such kind of abuse is voice spam, known as Spam over Internet Telephony (SPIT). Telemarketers, prank callers, and advertisers adopt VoIP for sending bulk unsolicited calls and messages. Such use of VoIP is made easy by the straightforward integration with current email spamming tools and the cheap calling rates available in the market. SPIT callers generate SPIT calls for various purposes: advertising products, convincing people to dial special expensive numbers, illicitly obtaining credit card information, and doing Voice Phishing (Vishing).

* *Corresponding author*. Tel.: +351 912691787.
E-mail addresses: muhammad.ajmal@fe.up.pt, majmalazad@gmail.com (M.A. Azad), ricardo.morla@fe.up.pt (R. Morla).
0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.07.006

In emails, social media sites, and blogs, spam is typically detected through black or white listing and message content processing. The black and white list may control the spamming activity but requires continuous update of list databases and some level of user interaction. Although content-based approaches have shown good detection performance, their application in a real-time voice network is not straightforward. 1) The contents are only available after session setup, when it is too late to prevent the spam call and the callee has already been disturbed with the call. 2) User privacy concerns, real-time speech processing, encrypted contents and legal issues also limit the application of content processing techniques to SPIT detection. Legitimate users tend to interact with their family, friends and colleagues. Non-legitimate users exercise massive spamming to a large number of users. These behaviors can reveal some interesting patterns that can be used to distinguish spammers from non-spammers. For example, telemarketers usually call or send messages to a large set of users to market their products. This behavior is very different from a legitimate user whose interactions are restricted to some social group. These communication patterns of users have been adopted to fight spam in email (Chirita et al., November 2005; Lam and Yeung, August 2007; Boykin and Roychowdhury, April 2005) and in social networking (Wang, July 2010). In the context of voice communication, call duration, the number of calls to a particular callee (called intensity), and callee feedback about the caller have been used for analyzing the communication behavior of a caller to detect SPIT (Balasubramaniyan et al., August 2007; Dantu and Kolan, July 2005; Sengar et al., 2012).

In this paper we propose Caller-REP (Caller-REPutation), a new approach to rank VoIP callers and detect SPIT without any content processing, user involvement, or changes to the VoIP network infrastructure. The main procedure is to process call detailed records (CDR) and create a social graph derived from the communication history of each caller. Our approach is based on two observations. 1) Legitimate callers tend to call the same numbers several times, to receive calls back, and to make longer rather than shorter calls (Seshadri et al., November 2008; Bokharaei et al., April 2011; Wilson et al., 2009) to a relatively large number of people. 2) Telemarketers and advertisers tend to have the opposite behavior: they try to call a large number of people to deliver their messages (Seshadri et al., November 2008; d'Heureuse et al., 2011) often resulting in short duration calls as the other party quickly hangs up after realizing that the call is spam. These callers also have fewer incoming than outgoing calls, as almost no one is interested in calling them back. In our approach, we propose to utilize CDR and the resulting social network to help distinguish between these kinds of proposed patterns and detect non-legitimate callers.

For each VoIP user in a network, Caller-REP first considers the neighbors of the user, i.e. other users he calls or receives calls from, and computes the direct trust a user has with the people he calls or receives calls from. The direct trust between caller and callee is computed with the following features: number of calls made or received, call duration in both directions, and the number of out-partners of a caller. The global reputation of a caller across the network is then computed through the power iteration method using the direct trust scores of a caller. Caller-REP favors callers that make long duration calls to a relatively small number of callees. Finally, Caller-REP takes the 25th percentile of the global reputation distribution as a threshold for classifying callers as SPIT or non-SPIT. Operators can change this threshold to adjust the false positive and false negative rates.

We evaluate the performance of our system by simulating the behavior of SPIT and non-SPIT callers. We do this for different network conditions including sparse networks and networks with different percentages of SPIT and non-SPIT traffic. The performance results show that our approach is more effective in detecting SPIT callers when the portion of SPIT callers in the network is below a threshold. In addition, Caller-REP yields no false positives under high SPIT rate. We also show that our approach outperforms state of the art SPIT detection.

The major contributions of our work are:

- Caller-REP, a new VoIP user social network-based approach for detecting non-legitimate callers. We do this without inspecting voice content and without asking caller or callee for feedback.
- New social network features for computing direct trust and global reputation in social network-based SPIT detection (namely node degree combined with call duration and call rate).
- A new detection method based on the 25th percentile that is used for discriminating SPIT from non-SPIT callers.
- An SPIT generation model with which a large range of synthetic VoIP usage behavior data can be produced. We evaluate the performance of Caller-REP using data from this model.

The remainder of the paper is organized as follows. In Section 2 we provide some background on SIP communication and SPIT. In Section 3 we discuss related work in the area of SPIT detection focusing on reputation-based systems. Section 4 provides background on social network features for developing Caller-REP. In Section 5 we detail the design of Caller-REP and describe the algorithms for computing direct trust, global reputation and automated threshold. Section 6 provides the simulation setup we used for evaluating Caller-REP. Section 6 provides the effectiveness of Caller-REP and its comparison with other detection methods. We briefly discuss the positive and negative aspects of Caller-REP and practical deployment issues in Section 8 and provide concluding remarks in Section 9.

2. VoIP (Voice over IP)

VoIP enables voice and multimedia communication to be carried over IP-based networks rather than the traditional Public Switched Telephone Network (PSTN). Enterprises and telephony service providers across the globe are adopting VoIP for its low cost. A VoIP session has two phases: a signaling phase and a voice transmission phase. VoIP transports signaling and voice over an IP network and is thus vulnerable to the security threats that affect IP networks. These attacks includes: Voice Phishing (Vishing), VoIP Spam (SPIT), scanning