2011 2nd International Conference on Networking and Information Technology
IPCSIT vol.17 (2011) © (2011) IACSIT Press, Singapore

A Study on Countering VoIP Spam using RBL

Seokung Yoon, Haeryoung Park, Myoung Sun Noh and Yoojae Won and Hyeong Seon Yoo

Internet Incidents Prevention Division, Korea Internet & Security Agency, IT Venture Tower, Jungdaero 135,
Songpa, Seoul, Korea , Department of Computer and Information Engineering Inha University 253,
Yonghyun-dong, Nam-gu, Incheon, Korea

Abstract. A threat of VoIP spam is becoming more and more actualized with the growth of VoIP service. Currently, most spammers send spam through internet telephony because they are possible to send spam in bulk and cheaply. Also, they could detour the most effective techniques currently in use for countering e-mail spam due to VoIP characteristics. RBL is one of the useful techniques to prevent e-mail spam and it also could be used to prevent VoIP spam. It is important to consider the attributes of VoIP call for adopting RBL in VoIP. This paper proposes a novel technique using RBL with six factors to calculate the spam score for countering VoIP spam.

Keywords-VoIP spam, RBL, VoIP call attributes, VoIP spam score

1. Introduction

VoIP (Voice over Internet Protocol) continues to be a growing service in nearly every country. Global growth of fixed-line VoIP services will double to $40bn by 2015 [1]. It is predicted to replace the PSTN in the near future. As VoIP service is revitalizing, the threats of VoIP service are also increasing. Therefore, it is necessary to provide PSTN-level security for continuous VoIP popularization

VoIP inherite security vulnerabilities from IP network and has new threats from its protocol such as SIP (Session Initiation Protocol) or H.323. VoIP spam is unwanted, automatically dialed, pre-recorded phone calls using VoIP, and it is one of the most serious threats in VoIP service [2]. It is possible to analyze the contents of e-mails before they are delivered to the recipient, but VoIP does not. This can lead to a weakening of the most effective means currently in use for countering e-mail spam [3].

In this paper, we propose a functional architecture to use RBL for preventing VoIP spam. We also define six factors to calculate VoIP spam score. The VoIP spam score is a quantitative value that reflects how malicious senders are. During call setup, each call is examined whether it already listed in RBL or not. Although a suspicious call is not listed in RBL, it will be blocked by calculating VoIP spam score. When the VoIP spam score of the call exceeds the threshold, it will be blocked and listed into the RBL.

The remains of this paper are as follow. In Section 2, we present a background of VoIP spam. In Section 3, we propose a functional architecture and a scheme for countering VoIP spam. In Section 4, we evaluate our scheme with experimental result, and we conclude this paper in Section 5.

2. Background

2.1. VoIP Spam

VoIP, like email and other Internet applications, is susceptible to be abused by malicious parties initiating unsolicited and unwanted communications. And, telemarketers, prank callers, and other telephone system abusers are likely to target VoIP systems increasingly.

One of the VoIP spam type is one-ring spam that a spammer cancels before call setup. When a recipient makes a call with displayed number, a spammer sends pre-recorded commercial messages to the recipient. In case of one-ring spam, there is no RTP media traffic transmission between the spammer and the recipient. Therefore, spammers could send VoIP spam without any cost.

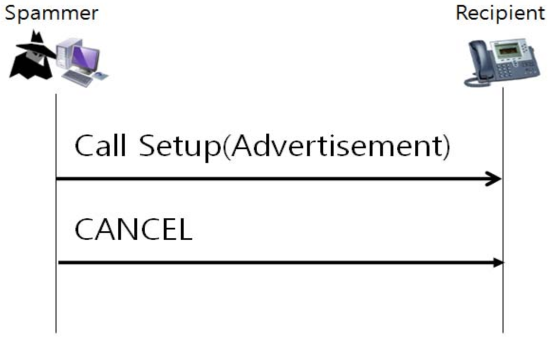

Figure 2. One-ring spam

One more spam type is that a spammer sends a commercial message (text or voice) via VoIP to the unspecified recipients at the same time. In real world it shows higher frequency than one-ring spam, spammer could send VoIP spam in bulk with less cost. But most recipients do not hear the commercial message to the end, call duration relatively short compare than normal call.

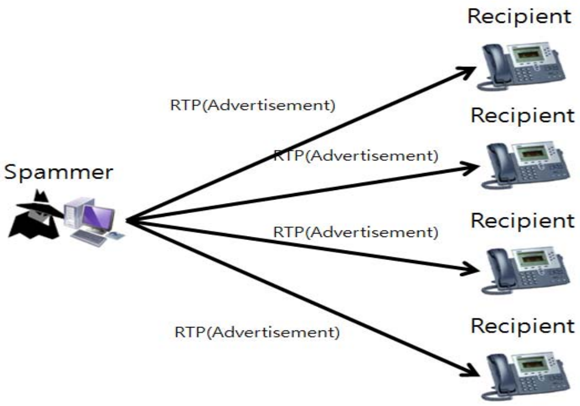

Figure 3. VoIP spam to unspecified recipients

2.2. Static and Dynamic attributes of VoIP calls

According to Kim, et al. [4], there are some characteristics that we should consider to distinguish a spam caller. They suggest identity strength and call cost as static attributes. Also, they propose that call duration is most important factor to calculate VoIP spam score. Also, inter-arrival time, recipient decision, contents and rejection rate are used to determine the main dynamic attributes in Table 1.

TABLE I. MAIN DYNAMIC ATTIBUTES OF VOIP CALLS

Attributes	Description
Inter-arrival time	Call creation cycle
Duration	Call keeping time
Recipient decision	Set destination of calls
Contents	Silence length of voice messages
Rejection rate	Failure probability of calls

3. Proposed Fucntional Architecture and Scheme

3.1. Overview

Functional architecture for countering SIP-based VoIP spam based on RBL is shown in Fig 2. It consists of two domains: outbound domain and inbound domain. Both domains contain sender and recipient respectively.

It also consists of three functional entities: Proxy, Policy server, and Reputation system. During call setup, each call is examined and blocked by RBL. Although a call which has spam characteristics is not blocked by RBL, it is examined by reputation system and blocked when VoIP spam score of the call exceeds the threshold.

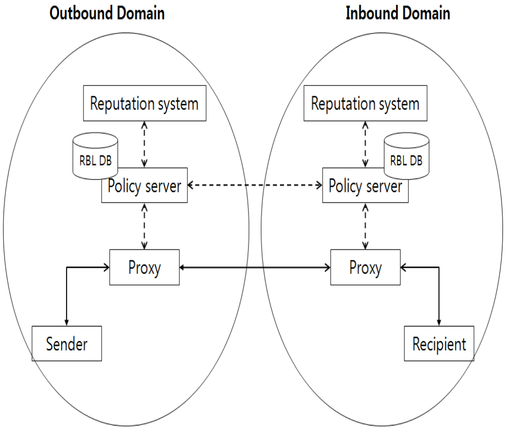

Figure 2. Functional architecture for countering VoIP spam

3.2. Functional Entities

- Proxy: The proxy blocks VoIP spam during call process using RBL. It can be implemented into the existing proxy server or call server in VoIP network
- Policy server: The policy server creates RBL and sends it to the proxy for blocking VoIP spam. It also exchanges its RBL with other policy server and updates its RBL. The proxy and the proxy server are logically separated but they can be implemented into one device
- Reputation system: The reputation system calculates VoIP spam score. For calculation VoIP spam level, six factors can be used.

3.3. Procedures

Procedures for countering SIP-based VoIP spam and updating the RBL are shown in Fig. 2.

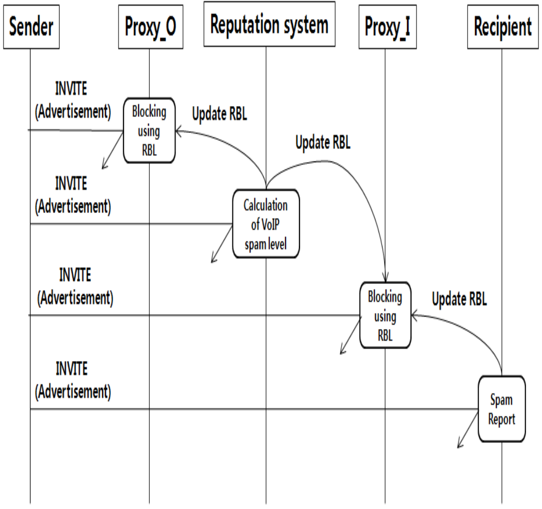

Figure 3. Anti VoIP spam procedure

- When a malicious sender sends INVITE message to recipient, the proxy of outbound/inbound domain checks its RBL receiving from policy server and blocks immediately if a malicious sender is already listed in its RBL
- Although the call from malicious sender is not block by proxy of outbound/inbound domain, call information is sent to the reputation system. The reputation system calculates VoIP spam level and

returns a result to proxy for blocking a spam call. If the VoIP spam level exceeds its threshold, the proxy blocks the call. After blocking it, policy server updates its RBL according to the result

- Otherwise, the call is delivered to one or more recipients. When a recipient realizes a spam call, he (or she) sends a spam report to policy server through proxy. After receiving it, policy server updates its RBL and the call from suspicious sender will be blocked

3.4. VoIP spam score

The VoIP spam score is a quantitative value that reflects how malicious senders are. A sender with a higher score is most likely to be a spammer. To calculate the VoIP spam score, we modified some factors defined in reference [4]. The six factors described in Table 2 are used as quantitative values.

TABLE II. FACTORS IN CALCULATING THE VOIP SPAM SCORE

Factor	Definition
Call Recipient Rate	The ratio of the number of recipients to the number of all attempted calls
Call Duration Rate	The ratio of the number of suspicious calls to the number of all attempting calls where a suspicious call is a call whose time duration is shorter than a certain value. For example, the call duration of suspicious call would be below 30 seconds because spammers generally make a call within 30 seconds
Average Call Traffic Rate	The ratio of the number of suspicious calls to the number of all attempting calls where a suspicious call is a call whose required bandwidth is more than a certain value. For example, if a sender generates traffic over 10% of average call traffic, the call is considered a suspicious call
Call Blocking Rate	The ratio of the number of blocked calls to the number of all attempted calls
Inter Call Time	Average time interval between the call attempts of a sender per unit time
Call Rate	Average call time when a caller makes certain number of calls. For example, the certain number should be bigger than 100.

- Call Recipient Rate
  1. Collecting recent 100 calls' info. of each caller
  2. Getting call recipient info.
  3. Exclusion of duplicated call recipient
  4. Deriving the number of call recipients
  5. Deriving call recipient number Rate

- Call Duration Rate
  1. Collecting recent 100 calls' info. of each caller
  2. Getting call duration info.
  3. Exclusion of calls having longer call duration than threshold
  4. Deriving the number of short length Calls
  5. Deriving call duration rate

- Average Call Traffic Rate
  1. Collecting recent 100 calls' info. of each caller
  2. Getting call traffic info.
  3. Exclusion of calls having shorter call traffic than threshold
  4. Deriving the number of call over traffic rate
  5. Deriving call traffic rate

- Call Blocking Rate
  1. Collecting recent 100 calls' info. of each caller
  2. Getting call rejection info.

3. Count corresponding caller's rejections
4. Deriving normal distribution of entire callers' call rejection count
5. Deriving the position of corresponding Caller's call rejection count over the accumulated normal distribution.

- Inter Call Time
1. Collecting recent 100 calls' info. of each caller
2. Getting Inter Call Time info.
3. Derive average of inter call time
4. Deriving normal distribution of entire callers' inter call time
5. Deriving the position of corresponding caller's ratio over inter call time average normal distribution

- Call Rate
1. Collecting recent 100 calls' info. of each caller
2. Deriving the range of time of corresponding caller's recent 100 calls
3. Deriving average of call rate
4. Deriving normal distribution of entire callers' call rate
5. Deriving the position of corresponding caller's call rate average over the normal distribution

4. Evaluation

4.1. Experiment Testbed

To test the VoIP spam detection function, we emulated spam calls by human. We used a VoIP phone numbered 6701 as a spammer. This phone attempted to make spam calls to the other VoIP phones numbered 6710~6789. We attempted to attack totally 2 times. At the first step, we tried to emulate one-ring spam. We tried to call 77 times to different recipients without answer. At the second step, we tried to emulate spam using automatic call system. We tried to call 63 times to different recipients, and each recipient answered the call, but finished it in 10 seconds.

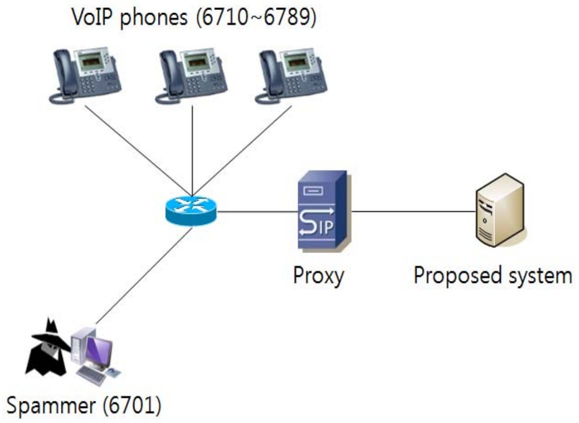

Figure 4. Diagram of the testbed

4.2. Experimental Result

The proposed system detected 88.3% of one-ring spam calls and 90% of automatic call system spam calls for the second test. And it recorded only 0.16% of false positive rate. The false positive rate is derived by the formula (1).

$$\text{False Positive Rate} = \frac{False\ positive}{Entire\ Calls} \times 100 \quad (1)$$

The proposed system miss detected only 5 calls out of 3,150 normal calls. And we expect that if the dataset get larger, it will get more detail information for detection, and false positive rate will be lower.

TABLE III. FALSE POSITIVE RATE OF SPAM TEST

Entire Calls	**False Positive**	**False Positive Rate**
3,150	5	**0.16%**

5. Conclusion

This paper proposes a technique to counter SIP-based VoIP spam using RBL. Our contribution is decreasing false positive rate of VoIP spam detection with six factors.

The proposed scheme is generally implemented as an independent server. It can also be implemented as modules of the existing proxy server. According to the experimental result, it could work as a practical VoIP-aware network security solution.

As future work, we need to consider weight of each factor to make the proposed system more efficient. And we will find the optimal value of weight to minimize the false positive rate.

6. Acknowledgment

This research was supported by the ICT Standardizationprogram of MKE (The Ministry of Knowledge Economy)

7. References

[1] http://unified.cbronline.com/news/voip-market-growth-to-hit-40bn-by-2015-report-160611.

[2] VoIP spam, http://en.wikipedia.org/wiki/VoIP_spam.

[3] ITU-T draft Recommendation X.1246, “RBL-based framework for countering VoIP spam”, April 2011.

[4] J.Y. Kim, H.J. Kim, M.J. Kim, Y.D. Cho, “VoIP spam call modeling using OPNET modular”, ACCS 68-73, August, 2009.