Computer Communications 42 (2014) 60–69

Contents lists available at ScienceDirect

Computer Communications

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

ICMP based IP traceback with negligible overhead for highly distributed reflector attack using bloom filters

S. Saurabh *, A.S. Sairam [1]

Department of Computer Science, Indian Institute of Technology, Patna, Navin Government Polytechnic Campus, Patliputra Colony, Patna 800013, Bihar, India

ARTICLE INFO

Article history:
Received 24 July 2013
Received in revised form 17 December 2013
Accepted 11 January 2014
Available online 23 January 2014

Keywords:
IP traceback
Distributed reflector attack
Denial of service attack
Bloom filter
Reverse iTrace

ABSTRACT

Most of the schemes that mitigate *DRDoS* attack only provide mechanism for filtering the attack traffic. They do not provide any tool for tracing back to the attacker. The few schemes that perform IP *traceback* requires involvement of the reflectors which is quite difficult to obtain. They require reflectors to store huge amount of traffic logs and cooperate during the attack. *Reverse iTrace* is one of the only methods that help in identifying the attack source without any involvement of reflectors. However, it generates huge amount of overhead traffic and does not scale well in case of large number of reflectors. These problems have discouraged its deployment in the Internet. In this paper, we propose a system of two bloom filters known as Additive and Multiplicative Bloom Filters, which when incorporated with Reverse *iTrace* reduces the number of iTrace generated approximately by 100 times. It also prevents *iTrace* from becoming another *DoS* attack during the reflector attack. Our system has Attacker Identification Probability of around 95%. Moreover, it is highly scalable. Extensive mathematical analysis and experimental results obtained from traffic traces prove the effectiveness and accuracy of our work.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

Attackers can render Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack more effective and difficult to traceback by making intelligent use of reflectors. IP hosts like web servers, DNS servers and routers that return reply packets for any request packet they receive can serve as reflectors. The attackers (slaves) send request packets to millions of reflectors with source IP address spoofed as that of victim. The innocent and unwitting reflectors upon receiving the request packets, send reply back to the victim. The combined effect of getting replies from these reflectors is that all possible paths to the victim gets flooded and hence it results in a distributed reflector denial of service (DRDoS) attack [1].

ICMP traceback based Reverse iTrace [1,12,13] is one of the only few schemes that can perform traceback (in case of reflector attack) without any involvement of reflectors. In this scheme, en route routers are induced to generate ICMP traceback messages, which are later used for IP traceback. However, ICMP traceback based schemes generate huge amount of overhead traffic even when there is no attack and they become the cause of another DoS attack while the reflector attack is going on. Due to the above mentioned reasons, these schemed have been rendered impractical for deployment in Internet.

In this paper, we propose two important modifications to the Reverse iTrace explained in Section 3.3, which almost eliminates the *overhead* traffic generated, while maintaining the same traceback success rate. To reduce the number of ICMP messages generated, we directly try to identify the source of the attack instead of trying to construct the entire attack path. The number of trace messages generated is further reduced by means of two novel bloom filters, Additive Bloom Filter (ABF) and Multiplicative Bloom Filter (MBF). These two bloom filters are used in series i.e., the output of ABF is fed as input to MBF. The additive bloom filter stops trace messages from being generated by legitimate traffic. The Multiplicative Bloom Filter bounds the number of trace messages packets generated by the attack traffic. The combination of these two filters help in generating ICMP traceback messages just at the start of an attack so that traceback is performed at the earliest with greater success rate.

1.1. Contributions

Main contribution of our work is: (a) We propose a *traceback* scheme for reflector attacks that directly identifies the edge router admitting attack packets. (b) The number of trace messages generated is reduced significantly by making intelligent use of bloom filters. (c) Trace messages are generated at the initial stage of an attack to facilitate early detection. (d) Our scheme is highly scalable. (e) We provide an in depth mathematical analysis of the system. We validate the analytical results with experiments which

* Corresponding author. Tel.: +91 612 2223538; fax: +91 612 2227050.
E-mail addresses: ssaurabh@iitp.ac.in (S. Saurabh), ashok@iitp.ac.in (A.S. Sairam).
[1] Tel.: +91 612 2552067; fax: +91 612 2277383.

0140-3664/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comcom.2014.01.003

were done using traffic trace files available from Umass Trace Repository [26].

1.2. Outline

In Section 2 we discuss the related work and explain why our system performs better than the present ones in performing IP traceback. Section 3 discusses about reflector attacks, ICMP traceback and Reverse iTrace. It also describes the problem statement along with important definitions and assumptions used in this paper. Section 4 discusses the proposed algorithm. Section 5 describes the parameter setting of our bloom filters. Section 6 gives the mathematical analysis for our system. Section 7 discusses the obtained results. Section 8 concludes the paper with reference to some future work.

2. Related work

Paxson [1] was one of the pioneers in the field of reflector attack. He observed that reflector attack traffic contains sufficient regularity and semantics to be easily filtered out. He proposed to filter those specific kinds of packets based on the attack signature. However, success of this scheme was based on system being updated with all the latest attack signatures. Otherwise, it could not work for unknown attacks.

To overcome the problem, Hiroshi et al. [7] proposed a method that monitored pairs of requests and responses at the edge router. It confirmed the validity of the received response packets based on the request response relationship. This method allowed response for packets only if their corresponding request was found. However, this method might not work in case of routing asymmetry where request and reply does not follow the same path. To overcome the routing asymmetry problem, Al-Duwairi et al. [6] proposed to validate incoming reply packets by pairing them, in a distributed manner, with the corresponding request packets. Pairing is performed at edge routers of ISP perimeter that contained the victim. However, coordination among the edge routers is difficult to obtain and might require a lot of message exchanges.

Works in [2,5] do not have any dependency on signature matching and matching between request-response packets. Wei et al. [2] proposed a protocol independent method to help in detection of most kinds of DRDoS attack. They observed that the rate of response flows from reflectors converging to the victim have linear relationship with each-other. Hence, they could differentiate reflected flows from legitimate ones efficiently and help in filtering *DRDoS* attack. In RAD [5], source AS marks packet with its Hash message authentication code (HMAC) and core routers filter packets that carry incorrect *HMAC*. Hence, a spoofed request packet will be filtered out at the edge router itself. However, success of this scheme is based on its complete deployment by each AS present in the Internet which is a big task.

Work by Husk and Vizvry [3] presents an analysis of a new kind of reflector attack orchestrated by using honey-pots as reflectors. They discuss the detection and filtering techniques of reflector attack from point of view of honey-pots. In [4], work is performed on detection of distributed denial of service attacks and reflector attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. NFBoost algorithm proposed in this paper achieves high detection accuracy (99.2%) and generates few false alarms.

The problem with all the above mentioned schemes is that they only perform detection and filtering of attack traffic but they do not perform IP traceback to catch the attackers and make them responsible towards law. Now, we survey some schemes that can perform IP traceback in case of reflector attack.

Belenky et al. modified deterministic packet marking (DPM) [25] to mitigate *DRDoS* attack and perform IP traceback. They suggested reflectors should have *DPM* logging enabled, so victim can get mark information from reflector's logs and trace slaves in *DRDoS* attack. Source Path Isolation Engine (SPIE) [19] records a set of hashes of packets traversing a given router. A victim can then traceback the path of a given packet by querying routers with the set of hashes corresponding to given packet. *SPIE* has the advantage that it can traceback by using just a single packet. However, it requires the routers in the path to log a lot of information which might not be feasible. ISP of reflectors might not be interested in cooperating in IP traceback because there is no immediate incentive and monetary benefit for them. Besides, traceback needs additional tasks like logging of packets, processing overhead and storage cost.

So we observe that most of the present schemes are able to detect and filter attack traffic in case of reflector attack [1–7] but very few perform IP traceback. Those which are able to perform traceback [19,25] need the cooperation and assistance of reflectors which is difficult to obtain. Major advantage of our proposed scheme is that it can perform IP traceback in case of reflector attack without any involvement from the reflectors.

3. Problem statement

3.1. Reflector attacks

A classical reflector attack is depicted pictorially in Fig. 1. The slaves send request packets to the reflectors, spoofed with the victim's IP address as the source address of packet. As a result the victim is swamped with huge number of reply packets from the reflectors. From the victim end, it is easy to locate the reflectors but much more difficult to traceback to the slaves. The operator at the reflectors, cannot locate the slaves as their source address is spoofed. They can, in theory, apply the traceback mechanisms that are available for DoS and DDoS attacks in order to trace back to the slaves. However if the traceback scheme is based on high traffic volume, as in case of probabilistic packet marking (PPM) [18] and iTrace [11], the use of reflectors make these schemes highly ineffective. This is because reflector attack diffuses the attack traffic and drastically lessens the number of packets sent from a single slave to different reflectors [2,5]. Hence due to insufficient number of packets, IP traceback cannot be performed for each slave–reflector pairs.

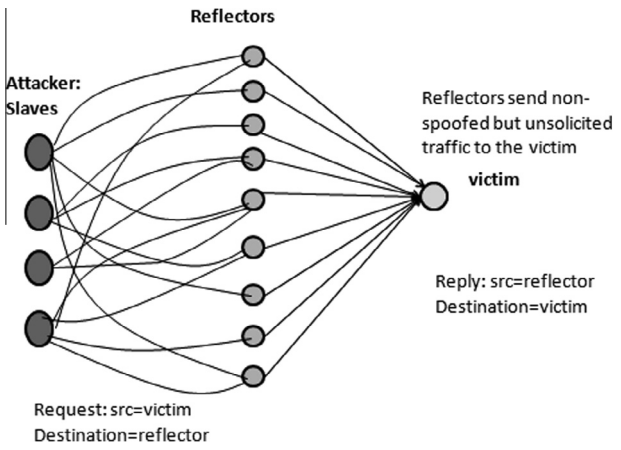

Fig. 1. Flooding based distributed reflector denial of service (DRDoS) attack. Slaves send spoofed requests (source = victim) to millions of unwitting reflectors which in turn send their combined replies back to the victim thereby causing flooding at the victim.

Download English Version:

https://daneshyari.com/en/article/450040

Download Persian Version:

https://daneshyari.com/article/450040

Daneshyari.com