ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 3, March 2013

Constructing IDPF to control IP spoofing based BGP updates

Sarika Dawakhar, Rajshree Kokate, Vijay Gadakh, Sagar Chavan

Student, Dept of Computer Engg, Sinhgad Academy of Engg College, Pune, India
Student, Dept of Computer Engg, Sinhgad Academy of Engg College, Pune, India
Student, Dept of Computer Engg, Sinhgad Academy of Engg College, Pune, India

ABSTRACT: IP spoofing remains a popular method to launch Distributed Denial of Service (DDOS) attacks. Several mitigation schemes have been proposed in literature to detect forged source IP addresses. Some of these solutions, like the inter domain packet filter (IDPF), construct filters based on implicit information contained in BGP rout updates. The packet filters rely on the fact that BGP updates are valid and reliable. This assumption is unfortunately not true in the context of the Internet. In addition, attackers can combine control and data plane attacks to avoid detection. In this paper, we evaluate the impact of false and bogus BGP updates on the performance of packet filters. We introduce a new and easy to deploy extension to the standard. BGP selection algorithm in order to detect spoofed BGP updates. The new proposal, credible BGP (CBGP), assigns credibility scores for AS prefix origination and AS path. These credibility scores are used in an extended selection algorithm to prefer valid BGP routes. Based on simulation studies, we prove that the proposed algorithm improves significantly the performance of
packet filters based on BGP updates.

Keywords: BGP, IDPF, IP Spoofing

I. INTRODUCTION

The lack of source IP address validation across multiple Autonomous Systems (ASs) in the internet makes it difficult to detect and prevent attackers from launching Distributed Denial of Service (DDoS) attacks using spoofed source IP addresses. Several popular internet sites [1] and internet infrastructure [2] have been attacked recently and such attacks have the potential to cripple the internet. Detection and prevention of these attacks is often made more complicated by attackers employing source IP address spoofing. The idea is to forge the source IP address in the "attack" packets to that of another host in the system. This allows the attacker to pose as some other host and hide its actual identity and location, making it difficult to detect the actual attacker and to protect against it.

II. IP SPOOFING DETECTION TECHNIQUE

The route based packet filter proposed by Park and Lee [3] relies on the basic fact that if a single-path routing scheme is assumed, there is exactly one single path p(s, d) between source node s and destination node d. Therefore, any packet with source address s and destination address d that appear in a router not in p(s, d) should be discarded. However, in order to construct a specific route-based packet filter at a node, it requires knowledge of global routing decisions made by all the other nodes in the network. Given the insular nature of how policies are applied at individual ASs, it is impossible for an AS to acquire the complete knowledge of routing decisions made by the other entire ASs. Hence constructing route-based packet filters as proposed in [3] is an open challenge in the current Internet routing regime. The IDPF architecture takes advantage of the fact that while network connectivity may imply a large number of potential paths between source and destination domains, commercial relationships between ASs act to restrict to a much smaller set the number of feasible paths that can be used to carry traffic from the source to the destination [4]. The packet is discarded if the check is negative. A key feature of the scheme is that it does not require global routing information.

III. SECURITY CONCERN IN BGP

BGP network design was undertaken in the relatively homogenous and mutually trusting environment of the early Internet. The underlying distributed distance vector computations rely heavily on informal trust models associated with information propagation to produce reliable and correct results. The approach to information exchange was not primarily designed for robustness in the face of various forms of negotiated trust or overt hostility on the part of some routing nodes in the network. BGP has several well-known vulnerabilities. These vulnerabilities are the direct

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 3, March 2013

consequences of three fundamental weaknesses in the BGP and the inter-domain routing environment [5]. The first weakness is there is no mechanism to check the integrity, freshness and source authenticity of BGP messages. Also, BGP doesn't offer any mechanism to verify the authenticity of an address prefix and an AS origination of this prefix in the routing system. Last, the BGP protocol doesn't provide any way to guarantee that the attributes of a BGP UPDATE message are correct. The lack of security concepts in BGP leaves it vulnerable to several types of control plane attacks. In addition, the IDPF scheme, which relies on BGP updates to detect and prevent source IP address spoofing, will fail if the BGP updates are not correct. The IDPF scheme assumes that BGP routing updates are secure and hence trustworthy. However, by accepting bogus BGP updates, the IDPF filters become less effective. The performance of IDPF scheme suffers when hostile nodes, which can generate non-trustable BGP updates and hence create incorrect filters, are introduced in the network (see section 5). This decline in IDPF performance can be arrested by deploying a mechanism to secure BGP. At present there are a number of practical and a number of more fundamental questions relating to securing BGP. The first is a practical question relating to the inevitable design trade-off between the level of security and the performance overheads of processing security credentials associated with BGP UPDATE messages. It is not entirely known as to what aspects of BGP performance and load are critical for the robust operation of network applications and what are not so critical. With such considerations, it is extremely important that any solution to secure BGP should try and minimize impact on current performance of BGP and should be incrementally deployable. Given this, there is a strong incentive to alter BGP such that it will provide reasonable amount of security at both control plane and data planes and will have minimal impact on BGP messaging .

IV. CREDIBLE BGP

Credible BGP calls for a modification to the standard BGP route selection algorithm such that it takes into account validity state of routing updates. These two scores are defined as follows:
Route origination validation score is derived based on the ability of a route receiving node to determine whether the AS originating the route actually is authorized to do so. Route AS-Path validation score is derived based on the ability to which the node is able to determine whether the received update actually traversed the ASs listed in the AS Path.

V. PERFORMANCE METRICS

False and bogus BGP updates have a significant impact on the performance of packet filters such as IDPF filter. In order to evaluate the impact of the proposed scheme on the performance of packet filters we introduce new performance metrics based on predefined set of metrics described in [3]. We define three metrics to measure the strength of the deployed solution to prevent IP spoofing attacks**.** Given the AS graph G= (V, E), we will use F to denote the sub-set F V of nodes where the new enhanced security scheme is deployed. We call μ=|F|/ |V| the coverage ratio.

We also define r as the ratio of spoofed BGP updates. *Sa,t* denotes [3] the set of nodes—more precisely, the set of IP addresses belonging to an AS node in *Sa,t*—that an attacker at AS *a* can use as spoofed source IP addresses to reach *t* without being cut-off by filters executed at autonomous systems in *T*. The larger the set *Sa,t*, the more options an attacker at *a* has in terms of forging the IP source address field with a bogus address which will go undetected. Whereas *Sa,t* is defined from the attacker's perspective, *Cs,t* captures the victim's perspective and denotes the set of nodes that could have sent an IP packet *M*(*s*, *t*) with spoofed source IP address *s* and destination address *t* which did not get filtered on its way. The larger *Cs,t*, the more uncertain the victim at *t* is upon receiving spoofed packet *M*(*s*, *t*) with respect to its true origin.

If |*Cs,t*| = 1, then this means that IP address *s* cannot be used by any attacker *a* (outside of *s* itself) to mount a spoofed DoS attack aimed at *t*.

Φ is defined as:

$$\Phi(\tau) = \frac{|\{t : \forall a \in V, |S_{a,t}| < \tau\}|}{|V|} \quad (1)$$

We define Φμ as:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 3, March 2013

$$\theta_{\mu}(r) = \frac{1}{|V|}\int_{1}^{|V|}\theta(\tau)d\tau \quad (2)$$

We define metric Ω to measure the average performance of IDPF in the presence of a variable rate of spoofed BGP updates. Ω is expressed as:

$$\Omega(\mu) = \int_{0}^{1}\Phi_{\mu}(r)dr \quad (3)$$

The enhancement of the effectiveness of IDPF in protecting ASes against spoofing based DDoS attacks is expressed as:

$$\lambda_{1}(\mu) = \frac{\Omega(\mu)}{\Omega(0)} \quad (4)$$

Similarly, AttackFraction denotes the fraction of ASes from which an attacker can forge addresses belonging to at most τ ASes, in attacking any other ASes in the network. Particularly, AttackFraction(1) is the fraction of ASes from which an attacker cannot spoof the IP address of any other AS to attack the network. is defined in [3] as:

$$\theta(\tau) = \frac{|\{a : \forall t \in V, |S_{a,t}| < \tau\}|}{|V|} \quad (5)$$

We define θμ as:

$$\theta_{\mu}(r) = \frac{1}{|V|}\int_{1}^{|V|}\theta(\tau)d\tau \quad (6)$$

θμ calculates the strength of IDPF in limiting the number of attackers in the presence of a percentage r of spoofed BGP routing updates in the network. We define as a metric to measure the average strength of IDPF filters in protecting the network against attackers .

Φ is expressed as:

$$\alpha(\mu) = \int_{0}^{1}\theta_{\mu}(r)dr \quad (7)$$

The enhancement of the strength of IDPF filter in limiting the spoofing capability of an arbitrary attacker is expressed as:

$$\lambda_{1}(\mu) = \frac{\Omega(\mu)}{\Omega(0)} \quad (8)$$

Last, the authors of [3] define a reactive metric Ψ that measures the effectiveness of IDPF in reducing the IP

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 3, March 2013

trace back effort, i.e., the act of determining the true origin of spoofed packets. Ψ is defined as:

$$\Psi(\tau) = \frac{|\{t : \forall s \in V, | C_{s,t} | \leq \tau\}|}{|V|} \quad (9)$$

We define δ_μ to measure the effectiveness of IDPF filters in determining the true origin of spoofed packets in the presence of a percentage r of spoofed BGP routing updates. δ_μ is expressed as:

$$\delta_\mu(r) = \frac{1}{|V|}\int_1^{|V|} \Psi(\tau) d\tau \quad (10)$$

The average effectiveness is defined as:

$$\beta(\mu) = \int_0^1 \delta_\mu(r) dr \quad (11)$$

The enhancement of the effectiveness of IDPF filter in determining the true origin of IP spoofing attacks is expressed as:

$$\lambda_3(\mu) = \frac{\beta(\mu)}{\beta(0)} \quad (12)$$

VI. PERFORMANCE OF IDPF FILTERS IN THE PRESENCE OF BGP UPDATES SPOOFING

In this section, we demonstrate how the performance of IDPF scheme declines in the face of growing number of bogus and false updates in the network. The graphs in Figure 1 to 3 demonstrate the progression of decline in the performance of IDPF scheme when an increasing percentage of untrusted BGP routing updates are introduced in the network.

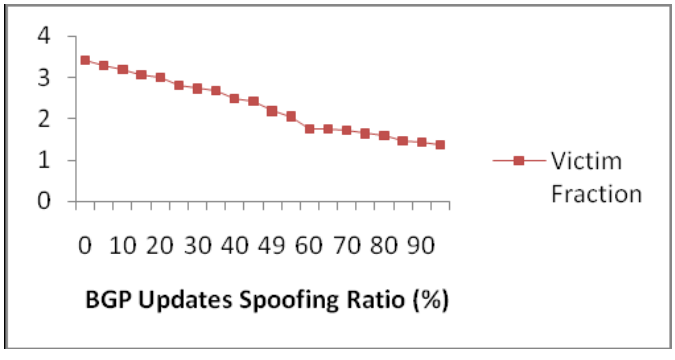

Fig. 1: Degradation of Victim Fraction Performance

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 3, March 2013

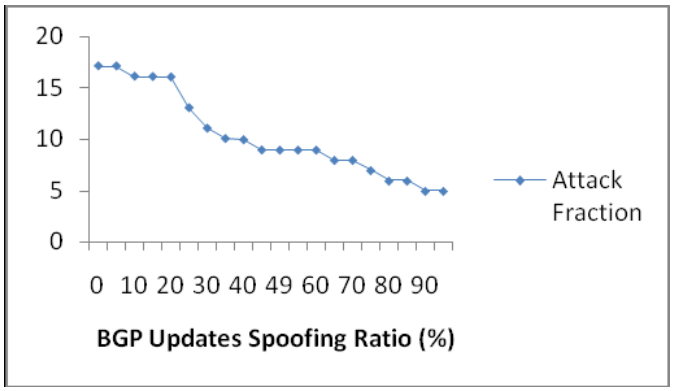

Fig. 2: Degradation of Attack Fraction Performance

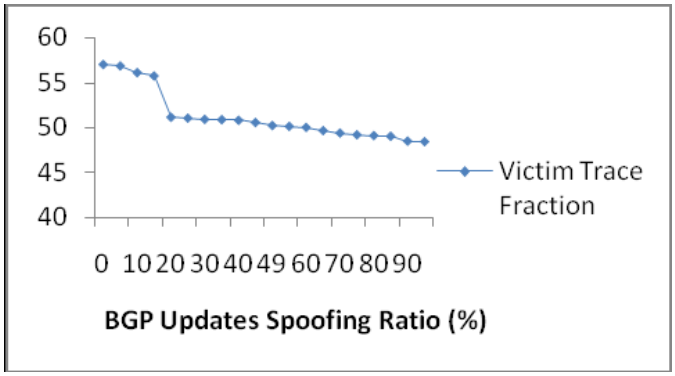

Fig. 3: Degradation of Victim Trace Fraction

The simulation results clearly demonstrate that there is a significant impact on the performance of IDPF filters when bogus and false updates are present in the network. Using this vulnerability in the IDPF scheme, attackers can combine both control plane and data plane to escape detection. It's obvious that the mitigation of IP spoofing attacks should be addressed on the control plane as well. In the next section, we will measure the enhancement of IDPF filters when Credible BGP is deployed in the network.

VII. PERFORMANCE GAIN RATIO OF IDPF FILTERS

Results from the previous section showed that there is a need to validate the BGP updates in order to ensure proper functioning of the IDPF filters. We have deployed CBGP increasingly in the network and measured the enhancement of the strength and effectiveness of IDPF filters. The new metrics $\lambda 1$, $\lambda 2$ and $\lambda 3$ measure the overall performance enhancement of VictimFraction, AttackFraction and VictimTraceFraction metrics respectively. Figure 4 shows the simulation results with a coverage ratio μ that varies from 0 to 100%.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 3, March 2013

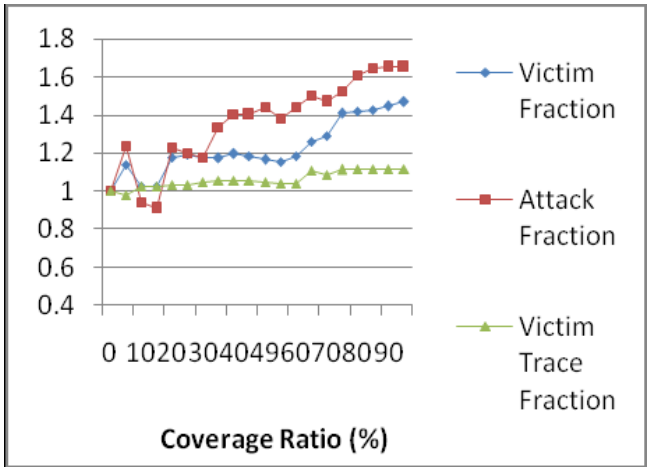

Fig. 4: Performance Gain Ratio of IDPF Filters

VIII. CONCLUSION

In this paper we proposed an easy to deploy protocol to validate BGP routing updates. CBGP modifies the current BGP selection algorithm by adding an extra check of the validity of the origin IP prefix and the AS path. We proved using simulation studies that the performance of packet filters based on BGP updates is improved when CBGP is deployed in the network. It would be interesting to determine the impact of the proposed change in BGP selection algorithm on the control plane load in the network. Since the proposed validity state factor will override other criteria for BGP decision process, the network routing table with the validity state factor considered will appear very different from when the validity state factor is not considered.

ACKNOWLEDGMENTS

This research was funded by a URP grant from Cisco Systems. The authors would like to thank David Ward of Cisco Systems for his support

REFERENCES

[1] Yahoo attributes a lengthy service failure to an attack. http://www.nytimes.com/library/tech/00/02/biztech/articles/08yahoo.html, February 2000.
[2] Massive DDoS attack hit DNS root servers. http://www.internetnews.com/entnews/article.php/1486981, October 2002.
[3] K. Park and H. Lee, On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets, In Proc. ACM SIGCOMM, San Diego, CA, August 2001.
[4] Y. Rekhter, T. Li, and S. Hares, A Border Gateway Protocol 4 (BGP-4), RFC 4271, Internet Engineering Task Force, January 2006.
[5] M. Dalal, Improving TCP's robustness to blind in-window attacks, Internet Draft, May 2005, Work in Progress.

BIOGRAPHY

Name	Affiliation
Rajshree Kokate Vijay Gadakh Sarika Dawakhar Sagar Chavan	Dept of Computer Engg, Sinhgad Academy of Engg College, Pune, India