Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.59 – 65

RESEARCH ARTICLE

An Integrated Approach to Detect and Limit IP Spoofing

Tanmay A. Abhang[1], Uday V. Kulkarni[2]
[1]M. Tech. Student, CSE Dept., SGGS IE&T, Nanded-431606, India
[2]Professor & HOD, CSE Dept., SGGS IE&T, Nanded-431606, India

[1] tanmay2abhang@gmail.com; [2] uvkulkarni@sggs.ac.in

Abstract— Transmission Control Protocol/Internet Protocol (TCP/IP) is the suite of communication protocols used to connect hosts on the Internet. IP address spoofing or IP spoofing is the creation of IP packets with a forged source IP address, with the purpose of hiding the identity of the sender or impersonating another computing system in order to gain unauthorised access. There are number of types of attacks that successfully employ IP spoofing. So it is mandatory for today's network scenario that there must be some mechanism present to avoid IP spoofing which ultimately causes different kinds of network and resource attacks. Many attempts are made to prevent from such attacks at router or network level. We employ an approach to control IP spoofing at Autonomous System (AS) level or at interdomain level by making use of implicit information contained in border gateway protocol (BGP) messages transferred between border routers of different ASes.

Key Terms: - IP spoofing; AS; BGP

I. INTRODUCTION

The term IP spoofing refers to creation of packets with forged IP address indicating that the message is coming from a trusted host. It is a complex technical attack that is made up of several components. It is a security exploit that works by tricking computers in a trust-relationship that you are someone that you really aren't. IP spoof attacks may occur after completion of authentication, allowing the attacker to masquerade as authorized user. By replacing the true originating IP address with a fake one a hacker can mask the true source of an attack or force the destination IP address to reply to a different machine and possibly cause a denial of service. Main purpose of such attack is to exhaust victim servers or saturating networks link. It leads to the interruption of services to known as Denial of Service (DoS). Distributed Denial of Service (DDoS) is type of DoS in which attacker attacks via bots dispersed all over the internet [1]. Based on victim, DDoS attack can be classified into two category a) Network resource attack and b) Server resource attack. In Network resource attack an attacker sends large number of useless packet in order to deplete the bandwidth of the link connecting network and the internet. In server resource attack attacker sends large number of packets to the server with intention to overload the victim server so that it can't process any packet further or consume all memory of the server.

IP spoofing allows the attacker to pose as some other host and hide its actual identity and location, making it inconvenient to pinpoint the actual attacker and to protect against it. In this scenario hosts or nodes that uses source address based filtering, proves to less effective in stopping attack. IP spoofing has become a foundation for launching various types of attacks and it will remain popular because the anonymity of attacker is preserved while victim is often is misled to innocent network or host. Many solutions have been proposed to avoid IP spoofing such as employing firewalls at routers, encryption at the session or secure server network layers with

SSL validation using 128-bit encryption are the primary protections against IP spoofing. The Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee have suggested some recommendation [2] to battle against IP spoofing problem. One of the most important recommendations is verification of source IP address which dictates the importance of the IP spoofing problem. IP spoofing is root cause of various attacks such as blind spoofing, man in the middle attack, TCP synchronous (TCP SYN) flood attack, SMURF attack, ping flood attack and distributed denial of service (DDoS).

II. RELATED WORK

Distributed change point detection (DCD) detects DDoS attacks at the traffic flow level using Change Aggregation Trees (CAT) [3]. DCD does so by detecting sudden traffic oscillations before they occur across inter domain network. Numerous authors have been worked on the problem to mitigate the level of IP spoofing in the internet. C. Jin *et al* have proposed Hop-Count Filtering (HCF) [4]. Idea behind HCF is that, though attacker can spoof arbitrary any IP address, he cannot forge or control the number of hops a packet takes to reach a network or host. Hence most of the packets with spoofed address will have a different hop count than legitimate packets hop count. A.Yaar *et al* in [7] described a deterministic packet marking mechanism in which a path identifier (Pi) is attached to each packet so that victim can know the path traversed by the packet. By attaching an identifier to each packet based on the router path that it traverse, victim can filter packet itself based on the path information carried by that packet. Suppose a router drops a packet because of spoofed address, it remembers the path identifier of the dropped packet and discards the entire subsequent packet traversing along path same as dropped packet or having same path identifier.

The Unicast Reverse Path Forwarding (uRPF) [5] feature helps to mitigate problems that are caused by spoofed IP source addresses into a network by discarding IP packets that lack a verifiable IP source. When uRPF is used, the source address of IP packets is checked to ensure that the route back to the source uses the same interface that the packet arrived on. If the input interface is not a feasible path to the source network, the packet will be dropped. Packet passport suggested by X. Liu *et al* [10] uses a lightweight message authentication code (MAC) such as hash-based message authentication code (HMAC) or message authentication code based on universal hashing (UMAC). A passport is nothing but a sequence of autonomous system (AS) numbers and their MAC's. MAC's are computed using a secret key known only to the source and passport checking domain between source and destination. Therefore passports cannot be forged by cryptographic methods. As packet travels from source to destination, routers between them validate the passport.

Source Address Validity Enforcement protocol (SAVE) [9] protocol when employed enforces all IP packets to carry correct source address. SAVE is based on the building an incoming table that consists of association of each incoming interface of the router with different valid source address block. If such tables are deployed at many routers, choices of spoofing addresses reduced to great extent. Route-based packet filtering [15] is discussed in next section.

Bremler *et al* proposed a spoofing prevention method (SPM) [11], where packets exchanged between members of the SPM scheme carry an authentication key associated with the source and destination AS domains. Destination checks each packets arriving for the authentication key. Packets with an improper authentication key with respect to the source are spoofed packets and are rejected.

III. IP SPOOFING DETECTION

Various techniques have been employed in order to limit the IP spoofing problem, one of the powerful technique is "route-based packet filtering". Idea behind route-based packet filtering is that, though an attacker can spoof any IP address, the path taken by a packet to reach the destination is not controlled by him [15]. Route-based routing assumes "single-path routing". It means there exist only a single path between a source '*s*' and destination '*d*' denoted by *p(s, d)*. Hence any packet having source address *s* and destined to *d* arrive at a router which is not in between the only path between *s* and *d* should be considered as spoofed and must be rejected. Exploiting this fact one can build a packet filter at a router to reject spoofed packet provided that this router must know the path from each source to each destination. Considering the size of today's network this idea seems to be very complex and unfeasible (about 44635 ASes).

Interdomain packet filter (IDPF) [14] is an attempt to overcome the issue of global routing information. IDPF basically works on route-based routing principle but instead of using global routing information, it makes use of inherent information from exchanged BGP messages in between the border routers. BGP is an exterior routing protocol which also is the de facto protocol for interdomain routing (in between AS). Every AS has one or more border router that exchanges information (import and export of best route to a destination) about its own network and other networks that it can reach. BGP is basically used for exchanging this reachability information. BGP is a policy based routing protocol [16], meaning there are some locally generated policies which governs

the acceptance (selecting a route) or forwarding (propagation of route) information. Therefore a physical connectivity between border routers of two ASes does not necessarily indicate reachability.

The locally generated policies are heavily affected by the contractual commercial agreement between ASes [17]. Every AS has its own set of policies irrelevant to the neighbor ASes therefore an AS cannot possibly gain knowledge of other ASes routing decisions. Taking into consideration these policies, though there can be large number of routes between any two nodes (source to destination) only some of them are actually used for carrying traffic in between them (feasible routes).

If ((u1 $if\ ((u1 \in customer(v) \cup sibling(v))$ $and\ (u2 \in peer(v) \cup provider(v)))\ then$ **r1.local_pref > r2.local_pref**

Fig. 1. Import policies

Export rules		**r1**	**r2**	**r3**	**r4**
Export to		**porvider**	**customer**	**peer**	**siling**
Learned from	**Provider**	No	yes	No	Yes
	customer	Yes	Yes	Yes	Yes
	peer	No	Yes	No	Yes
	sibling	Yes	Yes	Yes	Yes
Own routes		Yes	yes	Yes	Yes

Fig. 2. Export policies

Every router selects a single route from these feasible routes. If IDPF is enabled on a node say *a*, on receiving a packet *p(s, d)* on an interface from neighbor *t*, node *a* checks that if neighbor *t* has previously advertised a route to reach *s* or not. If *t* has advertised route then *a* accepts the packet otherwise the packet must be spoofed and *a* discards the packet.

IV. AUTONOMOUS SYSTEMS AND SIGNIFICANCE OF BGP

On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also known as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN). Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP). An autonomous system shares routing information with other autonomous systems using the Border Gateway Protocol (BGP). There exists a 3 relationships between two AS depending upon their commercial agreement [17].

a) Provider to customer relationship - a customer AS pays a provider AS which in turn carry traffic of customer AS to the rest of internet.
b) Peer to peer relationship - each AS in this relationship carry traffic from each other and their customers.
c) Sibling to sibling relationship - it is a special type of relationship in which each AS can be treated as others provider AS.

Internet service providers must use BGP to establish routing between one another. Therefore, even though most Internet users do not use it directly, BGP is one of the most important protocols of the Internet. A BGP router may accept NLRI (Network Layer Reachability Information) updates from multiple neighbors and advertise NLRI to the same, or a different set, of neighbors which is either announcement or withdrawal of a route. BGP maintains its own "master" routing table, called the Loc-RIB (Local Routing Information Base), separate from the main routing table of the router. For each neighbor, the BGP process maintains a conceptual Adj-RIB-In (Adjacent Routing Information Base, Incoming) containing the NLRI received from the neighbor, and a conceptual Adj-RIB-Out (Outgoing) for NLRI to be sent to the neighbor, means that the physical storage and structure of these various tables are decided by the implementer of the BGP code. Each BGP message consists of different attributes such as AS_PATH which is the sequence of ASes that this route has been propagated over, ORIGIN denoting where this message originated, LOCAL-PREF shows degree of preference for a path, COMMUNITY that can be applied to incoming or outgoing prefixes to achieve some common goal. Out of attributes stated previous we emphasize on AS_PATH and LOCAL_PREF attributes.

As discussed earlier the route selection and propagation process is dictated by locally defined routing policies viz. a) Import policies and b) export policies. Import policies which are applied before accepting route information while export policies are applied before sending route information to neighbors. Figure 1 shows import policy that suggest a router prefers a route learned from its customer or sibling over a route learned from its provider or peer AS. Figure 2 shows rules for export policies such as rule 1 indicates that a router will advertise routes to its own networks, routes learned from its customers and siblings to its provider, but will not advertise routes learned from its other providers and peers to the provider. Routing policy at an AS mainly depends upon the commercial relation between AS. A pair of AS can have provider to customer, peer to peer and sibling to sibling relationship. Every router selects and propagates to neighbors a single best route to the destination prefix. When a routing system is in stable state i.e. after exchanging several BGP update messages, all neighboring border router has updated information of each other's network reachability information and further exchange is halted till a router advertises update message. A router may receive NLRI for a certain prefix from more than one neighbor; in this case a router must decide which the best route among them is. This process is called as route selection process and it follows the rules given in fig. 3.

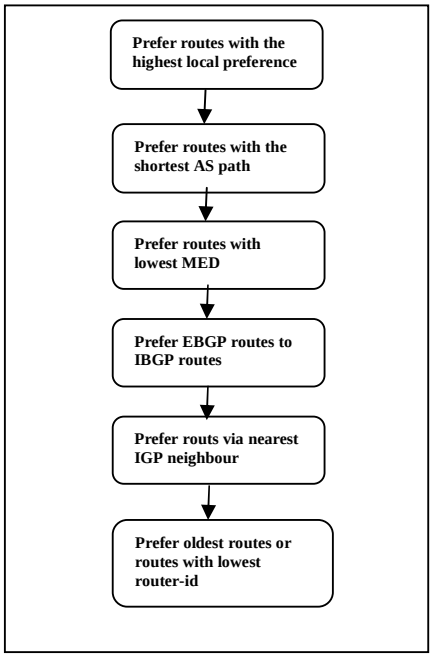

Fig.3. Route selection process

V. ENHANCED INTERDOMAIN PACKET FILTER (EIDPF)

Interdomain packet filter assures correct working in a scenario where certain conditions are satisfied such as system must be in stable state, system is strictly following import and export policies shown in fig. 1 and fig. 2 [12] Though network topology implies large number of paths between any two AS say a and b, business relationship between ASes greatly reduces the number of feasible paths that actually carry traffic. Border router chooses only a single best path from a set of feasible paths. IDPF certainly has advantage over route-based routing in terms of feasibility, as feasible routes can be easily calculated from BGP update messages while computing best path which needs global routing information seems to be impossible in current network scenario. Combining route-based routing with information obtained from BGP update messages, an interdomain packet filter is build. A feasible route is a topological route under BGP if it does not breach any routing policies imposed by the commercial relationship between ASes. If two routers are on the AS path back to back then they are said to be feasible upstream neighbor. Perception behind IDPF framework is: it is possible to calculate feasible upstream neighbor using BGP route updates. A router chooses a best route to network prefix from feasible routes; a node can only allow $p(s, d)$ from its feasible upstream neighbor to pass and rejects all other packet. So it guarantees that packets with valid source addresses are not discarded. It is shown by Z. Duan *et al*. [10], that when a routing system is stable i.e. after exchanging several BGP update messages, all neighboring

border router has updated information of each other's network reachability information and further exchange is halted till a router advertises update message. At this point the export policies employed by any router u is,

$$export\ (u \rightarrow v)\ [\{bestR\ (u, s)\}] \neq \{\ \}$$

It means that at stable routing each router sends its best route for reaching a node '*s*' to its each neighboring router. Provided that all ASes follows the import and export policies described in fig. 1 and fig. 2. It is obvious that a IDPF is less powerful than a route-based filter because IDPF are computed from feasible route from *s* to *d* and not from best route to reach *d* from *s*. Equipped with knowledge of feasible upstream neighbour and BGP messages received from it, we can now define interdomain packet filter as: a router *r* receives a packet *p(s, d)* from a neighbor *q*. Router *r* will accept the packet if and only if prior to reception of the same packet, *q* must have informed *r* about its best route to reach source *s*. Otherwise source address of the packet is forged and must be discarded.

Here only source address is considered before processing a packet. Constructing filter tables based on source address only instead of both source and destination, the per-neighbor space complexity for an IDPF node is greatly reduced from $O(n^2)$ to $O(n)$. Here n is the total numbers of border routers in related system. Working of IDPF can be said to be dependent on the Loc-RIB. Loc-RIB has entry for both neighbor peer and the prefix it has advertised or it can reach along with other attributes such as AS path, next-hop etc. Correctness of IDPF assured by the fact that it must not reject a single valid packet. EIDPF adds extra security to the existing IDPF architecture by integrating it with the ingress filter which provides increased intradomain security. EIDPF also does checking on false or bogus messages and rejects inappropriate BGP messages.

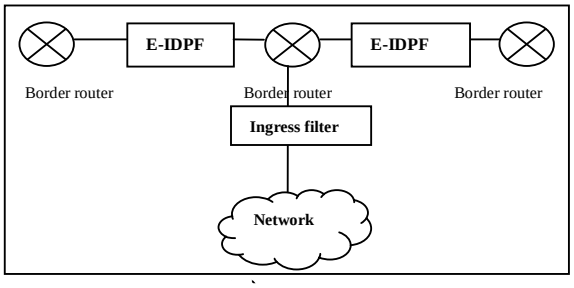

Fig. 4. EIDPF

EIDPF can be considered as interface specific packet-filter which is present on every interface of a router. Aggregating the process the EIDPF has following steps

I. If a packet is originating from network check its IP address
If it belong to network
Accept packet
Else
Reject packet
II. Select best routes to the different network prefixes using route selection process.
III. Update the Loc-RIB with best route information (if new).
IV. Infer feasible upstream neighbour from BGP update message for different network prefixes.
V. Receive packets from neighbour border routers.
VI. Check source address and calculate the network to which it belongs.
VII. If the same neighbour has previously informed about the network
Accept packet.
If not
Reject packet

EIDPF works complementary by adding more security and accuracy to IDPF by integrating it with ingress filters, in which traffic originating in a network is forwarded only if the source IP in the packets belongs to the network. We also provided additional checking to prevent false or bogus message exchange between border routers where a border router provides message of other routes as their own message.

VI. SIMULATION RESULTS

In order to simulate E-IDPF first goal was to create a scenario where different ASes are interconnected via their own border router and exchanges BGP messages in between them. Next aim was to obtain the Loc-RIB information of different border routers, processing information obtained from Loc-RIB to infer feasible upstream router and learn best route to a specific network prefix. Further define and construct IDPF based on collected information and test it to obtain results.

We performed simulations of AS level topology, using the state-of-the art C-BGP platform [20]. A system specifically designed to test EIDPF instead of using data set. We set up BGP policies according to the customer-provider, peer-peer relationships and we successfully checked the validity of the policies with the methodology as shown in [18]. The effectiveness of EIDPF is evaluated against both proactive and reactive capability. We took performance metrics introduced in [15] in our study and modified it according to the designed system to carry out results.

a) Proactive measure: - for any pair of ASes, say, *a* and *t*, $S_{a,t}$ is the set of Ases from which an attacker in AS a can forge addresses to attack . The larger the set $S_{a,t}$, the more options an attacker at a has in terms of forging the IP source address field without rejection.

b) Reactive measure: - For any pair of AS, *s* and *t*, $C_{s,t}$ is the set of ASes from which attackers can attack *t* by using addresses that belong to *s*, without such packets being filtered before they reach *t*.

We define two metric VictimRatio and VictimTracebackRatio that uses proactive and reactive measure respectively. Here, *V* is the total no of AS or node present in system.

$$VictimRatio = \frac{\{t : \forall a \in V, |S_{a,t}|\}}{V}$$

$$VictimTraceRatio = \frac{\{t : \forall s \in V, |C_{s,t}|\}}{V}$$

Deployment of EIDPF is an important issue. The results show that even if deployment of EIDPF at a single node reduces chances of IP spoofing significantly. It is obvious that if the AS deploying EIDPF is well connected, it can limit spoofing attack more efficiently and subsequently provides security to others ASes (in particular its customers) which are connected to it. So accepting EIDPF as a security can be a factor in receiving direct incentives. During test we place at different nodes (ASes) to check performance. First EIDPF at placed at feasible upstream neighbour and then later at well-connected nodes are selected.

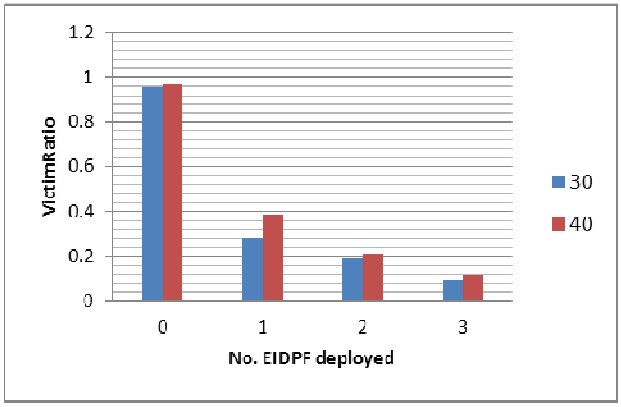

Fig. 5. Results for VicimRatio with different node coverage

Fig. 6. Results for VicimTraceRatio with different node coverage

VII. CONCLUSION

IP spoofing is a threat that can cause great damage in a network as it is being used as a tool in most of the popular attacks like DDoS, TCP SYN flood, SMURF attack etc. We have built EIDPF architecture to mitigate the problem of IP spoofing based on locally exchanged BGP updates. An ISP is suggested to employ EIDPF so that maximum networks are profited. Wide acceptance and use of these techniques is recommended as it will certainly increase the strength of network in order to fight against IP spoofing.

REFERENCES

[1] F. Baker, "Requirements for IP Version 4 Routers," RFC 1812, June 1995.

[2] ICANN SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks, Mar. 2006

[3] Yu Chen, Kai Hwang, and Wei-Shinn Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," IEEE Transcations on Parallel and Distributed Systems, Volume 18, Issue 12, pp 1649-1662, 2007

[4] C. Jin, H. Wang, and K. Shin, "Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic," Proc. 10th ACM Conf. Computer and Comm. Security, Oct. 2003.

[5] "Unicast Reverse Path Forwarding Loose Mode,"Cisco Systems, http://www.cisco.com/univrcd/cc/td/doc/product/software/ios122/122newf%t/122t/122t13/ft_urpf.pdf, 2007.

[6] The Swiss Education and Research Network. Default TTL values in TCP/IP, 2002. Available http://secfr.nerim.net/docs/fingerprint/en/ttl default.html.

[7] A. Yaar, A. Perrig, and D. Song, "Pi: A Path Identification Mechanism to Defend against DDoS Attacks," Proc. IEEE Symp. Security and Privacy, May 2003.

[8] A. Yaar, A. Perrig, and D. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense," IEEE J. Selected Areas in Comm., vol. 24, no. 10, Oct. 2006.

[9] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "Save: Source Address Validity Enforcement Protocol," Proc. IEEE INFOCOM, June 2002.

[10] X. Liu, X. Yang, D. Wetherall, and T. Anderson, "Efficient and Secure Source Authentication with Packet Passport," Proc. Second Usenix Workshop Steps to Reducing Unwanted Traffic on the Internet (SRUTI '06), July 2006.

[11] A. Bremler-Barr and H. Levy, "Spoofing Prevention Method," Proc. IEEE INFOCOM,Mar. 2005.

[12] P. Ferguson and D. Senie,Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing, RFC 2267, Jan. 1998.

[13] "CERT Advisory ca-1996-21 TCP SYN Flooding and IP Spoofing Attacks," CERT, http://www.cert.org/advisories/CA1996-21.html, 1996

[14] Z. Duan, X. Yuan, and C. Jaideep, "Controlling IP Spoofing through Interdomain PacketFilters," IEEE Transactions on dependable and secure computing, vol. 5, NO. 1, January-march 2008.

[15] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. ACM SIGCOMM,Aug. 2001.

[16] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, Mar. 1995

[17] L. Gao, "On Inferring Autonomous System Relationships in the Internet," IEEE/ACM Trans. Networking, vol. 9, no. 6, Dec. 2001.

[18] L. Gao and J. Rexford, "Stable Internet Routing without Global Coordination," IEEE/ACM Trans. Networking, vol. 9, no. 6, Dec. 2001.

[19] B. Quoitin, C. Pelsser, S. Uhlig and O. Bonaventure, "A performance evaluation of BGP-based traffic engineering", Wiley's International Journal of Network Management, Vol 15(3), p177-191, May/June 2005

[20] B. Quoitin and S. Uhlig, "Modeling the routing of an Autonomous System with C-BGP,",IEEE Network, Vol 19(6), November 2005.

[21] Z. Duan, X. Yuan, and J. Chandrashekar, "Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates," Proc. IEEE INFOCOM,Apr. 2006.

[22] C. de Launois, B. Quoitin and O. Bonaventure, "Leveraging Network Performances with IPv6 Multihoming and Multiple Provider-Dependent Aggregatable Prefixes," In Proceedings of QoSIP 2005, Catania, Italy, February 2-4th 2005

[23] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," Proc. ACM SIGCOMM Computer Comm. Rev., vol. 30, no. 4, Oct. 2000.

