IP Spoofing Defense: An Introduction

Lee Soon[a], Mohamed Othman[b], Nur Izura Udzir[c]

Department of Communication Technology and Network
Universiti Putra Malaysia, 43400 Serdang, Selangor
E-mail :[a]leesoon3@gmail.com, [b,c]{mothman,izura}@fsktm.upm.edu.my

ABSTRACT

In current Internet communication world, validity of source IP packet is and important issue. The problems of IP spoofing alarm the legitimate user of the Internet. This paper review recent progress of spoofing defenses by various researchers. Techniques and mechanisms proposed are being categorized to better illustrate the deployment and functionality of the mechanism. Overall, this paper summarizes the current anti spoofing mechanism in the Internet.

Keywords

IP Spoofing, IP Spoofing Prevention,IP Spoofing Defense, Network Security

1.0 INTRODUCTION

The basic protocol for the Internet communication is Internet Protocol (IP). Each IP packet has its own header with necessary felds that indicate the source and the destination of the packet (Postel, 1981). These felds are pre-format by the operating system before the packet is sent. If the source address of the packet header is forged, the packet will be seen as it was sent from other source. Forgery of IP packet is called IP spoofng. This hijacking technique used by attacker to mask their identity. IP spoofng is usually used on Distributed Denial of Service (DDoS), sending of spam and phishing mails attack.

IP spoofng had been a problem without easy solution. Attacks such as DDoS and TCP SYN flood base on spoofed IP had clogged the network. Phishing emails cost victims loses of money and phisher is left untraceable. These problems are urge to be solved. There are several ways for spoofng defense. We can categorize these mechanisms base on spoofng prevention before the transmission, spoofng detection during transmission and spoofng detection after it reach the destination.

2.0 Review of Spoong Prevention Before Transmission

In Network Ingress Filtering (Ferguson & Senie, 2000), authors proposed that, the traffic is forwarded if the source IP of the traffic is belongs to the network. Ingress Filtering will need a long period of time to be deployed on the Internet. Ingress Filtering prevents specific network from being used as victim of forged network address, however it did not address the problem of sending spoofed packet out to the network. Ingress Filtering will require every node within a network to deploy it, before it can work. Furthermore, routers will require additional configurations and filtering overhead.

3.0 Review of Spoofing Detection During Transmission

Route-based filtering (RBF) further extend network ingress filtering by filtering packet base on network topology. RBF autonomously harvest data traffic of suspicious source and update when there changes in route or routing table (Mirkovic, Jevtiv & Reiher, 2006). Author's work was separated into 2 parts: populating incoming table entries and updating them when routing changes occur, and filtering spoofed packet using incoming table information and ingress filtering. Author design Clouseau system to handle the first part and RBF handle the second part. Clouseau system randomly drop TCP data packet that arrive at router and observe subsequence retransmission from the same source. RBF at the same time filter spoofed packets by comparing packet's incoming interface with expected interface.

Consider two router, *A* and *B* connected to router *P*, and router *P* connected to router *R* through interface 2. Router *R* holds routing information of all incoming traffic that enters *R*. Traffic that comes from *A*, *P* and *B* will appear from the same interface 2. Author stated that if *P* and *R* both were filters then spoofing will be able to be detected.

RBF will works well for smaller network, but for the complexity of current architecture of the Internet, RBF will not scale. It will also be a problem for RBF to detect spoofed packet for a multihomed network and autonomous systems (AS). If the spoofed packet is sent and route from one network through another network, the packet will be detected as it come from another interface.

In Spoofing Prevention Method (SPM), router that is closer to the destination of a packet verifies the authenticity of the source address of the packet (Bremler-Barr & Levy, 2005). Routers mark and check outgoing packet with labels related to destination. An encrypted unique temporal key is associated with each ordered pair of source and destination network. The key is known in advance by both parties, and used as lightweight authentication mechanism to authenticate source address of incoming packets. Keys are placed when the packet is sent out from the router and being removed after the key of the packet is authenticated (at incoming router). When ISP detects attack on its network, they protect themselves by allowing only packets that come from SPM member network to ensure clean traffics.

The key player of SPM is the encrypted key placed on packets. In the paper, author suggested to place the key on packet's IP header; in IP option field or ID field. Author also suggested placing tagging task at edge routers at the ISP.

SPM has major advantage over RBF that SPM is an end-to-end protocol and require lower deployment cost, while RBF can only work (efficiently) if all ASes implement RBF. But SPM will only work if the source and destination of the (spoofed) packet is SPM router. Spoofing detection will not work if either side is not SPM router.

In Distributed Packet Filtering (Park & Lee, 2001) authors show that they can limit IP spoofing based on global routing information. Route based Distributed Packet Filtering (DPF) is placed on routers at vertex cover of AS network. Every router maintains a route and filtering table. Assume a packet is to be send from source *S* to destination *D*. When the packet enters the router of network from S, a set of feasible routes is being computed. Base on the routing policy, the best path is being chosen. In DPF, the shortest path is being implemented into the policy. The path from *S* to *D* is being maintained in router's route table. The incoming interface of the packet enters is checked when the packet arrived, by looking up into the routing table. If packet arrived from unexpected interface, the packet will be dropped.

Route based DPF is able to trace attacker's source AS with only one spoofed packet arrived at the victim. For tracing back attacker's location, route based DPF is able to minimize the possible attacker's origin network up to a very small range of network. Park's work shows that they can limit IP spoofing but it has some implementation issue; the scope of the work is too big. It is impossible to get all ISP around to world for it. Updating and maintaining the routing table (precisely) will also be a problem.

Duan, Yuan and Chandrashekar (2008) proposed an interdomain packet filter (IDPF) architecture based on on locally exchanged Border Gateway Protocol (BGP) updates only (p.22), as extension of DPF (Park & Lee, 2001). BGP works base on trust between ASes (Rekther, Li & Hares, 2006). BGP routers will update their routing table when they receive update message from neighbor node. In the process of deciding transmission route in BGP, when node *u* (AS router) receives an incoming packet forwarding request from neighbor node *W*, *u* will examine the destination of the packet. *u* will then import feasible routes to the destination from neighbor node. From all feasible routes, *u* will compute for candidate routes and choose the best route. *u* will then export the best route to *W*.

Whenever a packet enters the Internet, the router will check for the destination of the packet. IDPF gets feasible route from source node to the destination node through BGP transmission. Candidate routes and best route was chosen by IDPF base on their policies. In IDPF, AS nodes *v* will accept packet if and only if the packet come from neighbor node and that router is within the best route, otherwise the source address of the packet is spoofed. However, IDPF is not able to filter spoofed IP packet that is sent within the path of ASes the packet traverse. Spoofed packet will still be forwarded as any legitimate packet. Furthermore, IDPF only learn feasible routes, not the actual route the packet traverse.

Filtering of IP Spoofed Packets near the attacker (FSN) detects attacks based on information collected through Interior Gateway Protocol (Ohtsuka, Nakamura, Sekiya, & Wakahara, 2007) Outgoing packet at FSN router is marked with its own signature before forward to the next router. Neighbor Link Table (NLT) is constructed from topology information of link-state routing protocol. NLT contains information about source network, previous FSN router and router interface. Spoofed packet detection is performed by querying packet signature from NLT. Author proposed another approach with the same method under Open Shortest Path First (OSPF).

Source Address Validation Enforcement (SAVE) is a new protocol proposed to provide information needed to validate source address of incoming packet (Li et al, 2009). Each router that the packet traverse build correct incoming table with incoming interface. With this incoming table, each router can verify the packet and filter packets with mismatching source address.

SAVE provides end-to-end anti spoofing mechanism. Each router sends updates to neighbor router from time to time to update each other's incoming table like BGP and Routing Information Protocol (RIP). SAVE update records the path the update had traversed and assure that the update message traverse through the correct path. RBF limits the range of IP addresses for possible spoofing attacks but spoofing attack is still possible. IDPF and SAVE further improved RBF by forwarding packet only if they came from the correct interface.

Packet forwarding with source verification was proposed to address spoofing prevention via two approaches (Shue, Gupta & Davy, 2008). In the first approach, definitive packet tagging, routers tag packet that originate from their domain. Along the path that the packets traverse, the tag of packet will be verified. Once verified, the valid packet will be re-tag with the tag of the forwarding router. This hop-wise tagging process will keep the number of tag each implementing router has. Packet that is lack of tag or incorrectly tagged is dropped. The second approach, deductive packet tagging, implementing routers can verify and tag packet from nearby domain. Implementing routers involved in TCP handshake process from random routers to verify the tags.

Similar to source verification method, BGP Anti-Spoofing Extension (BASE) combines the mechanism of DPF (Park & Lee, 2001) and Path Identifier (Yaar, Perrig & Song, 2003). BASE filter packets base on their path tag (Lee, Kwon, Hasker & Perrig, 2007). Packet is tagged by a hashed marking value of their BGP path that is distributed using BGP updates. Every packet from the same source address will have the same tag regarding the path they traverse and interface they arrive from.. When a packet arrived at BASE deployed router, the router will tag outgoing packets and drop incoming packet without proper tag.

Unicast Reverse Path Forwarding (uRPF) require that the traffic is forwarded only if the traffic arrive at the same interface as the one that is used by the router to reach the source in forwarding table (Cisco Systems, 2005; Cisco Systems, 2007). Although the mechanism is simple, the effectiveness of uRPF is limited. With current architecture of the Internet, a lot of multihomed network have different interface for incoming and outgoing traffic. Traffic might traverse different path and uRPF require extra lookup at the router's forwarding table for each packet that arrive at the router. The efficiency of RPF depends on BGP routing information. RPF will drop valid packet if the router does not receive routing information BGP updates for the source prefix.

In Spoofing Prevention based on Hierarchical Coordination Model (SP-HCM), each ordered pair of source and destination network have a unique temporary signature (Lv & Sun, 2007). Similar to SPM (Bremler-Barr & Levy, 2005), routers in ASes mark outgoing packet with the signature. Upon arrival of packet at border router, the signature is being examined and verifies the authenticity of its source address. Source address information is transmitted by Hierarchical Coordination Model (HCM) using dynamic bloom filter. In SP-HCM, node of AS have sensor that continuously perform tasks by querying routers' Management Information Base (MIB) through Simple Network Management Protocol (SNMP) to gather information about managed entities. Actuator at border routers will poll for information from sensor and process it. Network address space signature is exchanged this way. Similar problem as SPM appears. SP-HCM will only work if all ASes deploy SP-HCM mechanism.

4.0 Review of Spoofing Detection at Destination

Wang, Jin and Shin (2007) proposed defense against spoofed traffic base on the value of Time To Live (TTL) on packet and compute the total hop the packet traveled from the source (attacker) to destination (p. 40). This value is very accurate as the value of TTL on a packet is not forgeable by attacker. TTL field of an IP header specify the maximum lifetime of an IP packet. Routers perform decrement by 1 on TTL when forwarding the packet to the next router. When a packet arrives at destination, TTL is subtracted with the initial value of TTL to get the total number of hop the packet traverse. Author built Hop Count Filtering (HCF) at end host, an accurate IP to hop-count (IP2HC) map by grouping IP prefixes based on hop count. In this case, TTL place the same role as temporal key in SPM, to authenticate packets that arrived at destination.

The effectiveness of HCF lies on the hop-count values of packet. HCF cannot detect spoofed and legitimate packets with same hop-count. Base on author's work, author suggests that spoofed IP packets have mismatch IP address and hop-count (base on IP2HC). By performing a lookup in IP2HC map HCF is able to drop spoofed traffics. HCF is believed to work well as attacker is not able to falsify the value of TTL, but intermediate attackers will be able to try to launch attack from location with matching hop-count values.

HCF causes delays to transmission. To overcome this problem, HCF operates under alert mode to detect spoofed traffic and action mode to drop packets when spoofed traffic is detected. Action mode will perform per-packet hop-count computation and compare with values in IP2HC. HCF is deployed at end host, hence easier to deploy compare to RBF.

Path Identifier (Pi) proposed a packet marking algorithm to mark each packet that traverse through Pi enabled routers onto the packet's header in IP Identification field (Yaar et al., 2003). The IP Identification field is broken into 16/n sections. When ever a packet enter Pi enabled router, the router compute the value of current packet's TTL modulo 16/*n* and insert into the IP Identification field before the packet is being forwarded.

Pi act as a fingerprint of the packet. Packets traveling the same path will have the same Pi value. Since it's a per-packet marking mechanism, victim will be able to defense himself from DDoS attack by filtering packets that carry the same Pi as attacker's packet. Pi works well under the network where all routers deploy Pi marking scheme. Unfortunately, it is rather impossible to have all routers in ASes from different ISP to deploy Pi. Furthermore, performance of Pi degrades when there are non-Pi enabled routers in between the path. These legacy routers will forward packets without marking them. Also the authors identified the problem of Pi where TTL is vulnerable to attacks.

StackPi by Yaar, Perrig, and Song (2006) improved Pi's performance by proposing two new marking schemes – Stack-based marking and Write-ahead marking (p. 1853). StackPi treat IP Identification field as a stack. When a packet enters a StackPi router, it left shift the value of IP Identification field for *n* bits and mark (push) its own marking bit into the stack. For packets that arrived on legacy router, the packet will have no interaction with the marking and forwarded. For routers that have the IP address of the next-hop, the router computes the marking bit for the next router and push into stack. This Write-ahead marking increase the performance of StackPi against legacy routers. StackPi's mechanism also increase the performance of HCF is being implemented together.

Gao and Ansari (2007) enhanced Pi's idea and introduced AS-based Edge Marking (ASEM) to marks packet at AS level (p. 732). ASEM only marks incoming packet on edge routers. All incoming packet is being marked with its AS number (ASN) of the edge router it enter. AS path is claimed to be shorter than IP path, hence address the problem of Pi. Pi limits the number of Pi mark to be store in IPv4 header to 16 bits, while the estimated size of Internet will require 28 bits to store Pi for end to end host. AS level marking is also more stable compare to IP level marking.

Chen, Park and Marchany (2007) proposed Attack Diagnosis (AD), which applies divide and conquer strategy in tracing packet source (p. 577). AD is divided into two paradigms. Attack detection on near victim's host is being performed. Once attack is detected, it will notify upstream routers to start marking incoming packets with interface port identifier (PID) for traceback. Based on the marking of packet, victim separate attacker's traffic from other client's traffic and notify upstream router to filter packets. AD have lower processing overhead compare to other proposed method as routers mark packet only after attack is detected. This is also the down side of AD as attack reached end-host, damage is occurred.

The above discussion is summarized as table 1.

5.0 Conclusion

This paper had reviewed different type spoofing defense mechanism proposed by various researchers. This studies shown that most researchers try to deploy spoofing defense during packet transmission, as a credit to customer and the ISP that implement it. Network Ingress Filtering works effectively but it only prevent its own network from spoofing, rather than protection its own network from being spoofed. On the other side, spoofing defense at the destination might introduce new problems other than anti spoofing.

Table 1: *Evaluation Parameter and Test Data for different method.*

Author	Method	Evaluation Parameter	Test Data
Park & Lee, 2001	DPF	Proactive & Reactive filtering on loose and tight mode	RouteViews Project
Yaar et al., 2003	Pi	No. of bits per router mark No. of hops away from the victim	Burch & Cheswick Internet Mapping Project
Bremler-Barr & Levy, 2005	SPM	Attack rate under no defense Attack rate under different filtering combination	Fixedorbit, IP address statistic
Yaar et al., 2006	StackPi	user acceptance ratio attacker acceptance ratio	Burch and Cheswick's Internet Mapping Project
Mirkovic et al., 2006	RBF	No. of source and unfiltered spoofed addresses for a given target destination No. of source and spoofing target for a given unfiltered spoofed address Spoofability of unfiltered spoofed addresses for a given source and target destination	RouteViews Project
Ohtsuka et al., 2007	FSN	Successful IP Spoofed Packet Detection Rate	Network Topology from BRITE
Gao & Ansari, 2007	ASEM	The number of packets required for path reconstruction	Skitter project of CAIDA & the Internet Mapping data from Lumeta
Chen et al., 2007	AD	false positive ratio Number of throttled attackers over time	Skitter project of CAIDA & the Internet Mapping data from Lumeta
Lee et al., 2007	BASE	Dropping ratio of attack packets Dropping ratio of legitimate packets	RouteViews Project
Lv & Sun, 2007	SP-HCM	Storage cost comparison for multiple-domain topologies	Transit-stub graph from GT-ITM
Wang et al., 2007	HCF	Filtering Accuracy Percentage of saved CPU cycle	DDos Testbed
Shue et al., 2008	Packet forwarding with source verification	Percentage of networks that are able to spoof Percentage of networks that can steal a tag Percentage of networks that can abuse a tag	Transit-stub graph from GT-ITM
Duan et al., 2008	IDPF	Victim Fraction Attack Fraction Victim Trace Fraction	RouteViews Project
Li et al., 2009	SAVE	SAVE Effectiveness Storage cost comparison for multiple-domain topologies Bandwidth ratio	Transit-stub graph from GT-ITM

Deploying spoofing defense during transmission seems promising with acceptable overhead and deployment cost, but there's an obstacle ahead – The Internet itself. The architecture of the Internet is consists of thousands of ASes. Each AS contains collection of connected IP routing prefixes under the control of routers of Internet Service Provider (ISP) with defined routing policy to the Internet. ASes of the Internet communicate with each other, maintain reachability and route traffics via various type of routing protocol.

Routing protocol keeps on evolving. With different routing algorithm and techniques, it is hard to implement a single spoofing defense mechanism that works with everyone. With IP multicast routing, mobility network and multihomed network, it further complicate the effort to deploy spoofing defenses effectively.

REFERENCES

Bremler-Barr, A. & Levy, H. (2005). *Spoofing Prevention Method.*

Chen, R., Park, J.M. & Marchany, R. (2007). A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks. *IEEE Transactions on Parallel and Distributed Systems, 18* (5), 577-588.

Cisco Systems (2007). *Unicast Reverse Path Forwarding* (Technical report). Retrieved from http://www.cisco.com/en/US/docs/ios/11_1/feature/guide/uni_rpf.pdf

Cisco Systems (2005). *Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider* (Technical report). Retrieved from http://www.cisco.com/warp/public/732/Tech/security/docs/urpf.pdf

Duan, Z., Yuan, X. & Chandrashekar, J. (2008). Controlling IP Spoofing through Interdomain Packet Filters. *IEEE Transactions on Dependable and Secure Computing, 5* (1), 22-36.

Ferguson, P. & Senie, D. (2000). *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, rfc2827* (Technical report). Cisco Systems, Inc.,13625 Dulles Technology Dr.,Herndon, Virginia 20170 USA: Cisco Systems, Inc. and Amaranth Networks Inc.

Gao, Z. & Ansari, N. (2007). A practical and Robust Inter-domain Marking Scheme for IP Traceback. *Computer Networks: The International Journal of Computer and Telecommunications Networking, 51* (3), 732-750.

Lee, H., Kwon, M., Hasker, G. & Perrig, A.(2007). *Base: An Incrementally Deployable Mechanism for Viable IP Spoofing Prevention.*

Li, J., Mirkovic, J., Ehrenkranz, T., Wang, M., Reiher, P. & Zhang, L. (2009). Learning the Valid Incoming Direction of IP Packets. *Computer Networks: The International Journal of Computer and Telecommunications Networking, 51* (2), 1389-1286.

Lv, G.F. & Sun, Z.G. (2007). *Towards Spoofing Prevention based on Hierarchical Coordination Model.*

Mirkovic, J., Jevtic, N. & Reiher, P. (2006). *A practical IP Spoofing Defense through Route-based Filtering* (Technical report). University of Delaware.

Ohtsuka, T., Nakamura, F., Sekiya, Y. & Wakahara, Y. (2007). *Proposaland Eficient Implementation of Detecting and Filtering Method for IP Spoofed Packets*

Ohtsuka, T., Nakamura, F., Sekiya, Y. & Wakahara, Y. (2007). *Realization of FSN Method for Detecting IP Spoofed Packets by making use of OSPF* (Technical Report 577). The University of Tokyo,2-11-16 Yayoi bunkyoku Tokyo, Japan: Graduate School of Frontier Sciences.

Park, K. & Lee, H. (2001). *On the Effectiveness of Route-Based Packet Filtering for Distributed Dos Attack Prevention in Power-Law Internets*, Vol. 31.

Postel, J. (1981). *Internet Protocol* (Technical report). University of Southern California, 4676 Admiralty Way, Marina del Rey, California 90291: Information Sciences Institute.

Rekther, Y., Li, T. & Hares, S. (2006). *A Border Gateway Protocol 4 (BGP-4)* (Technical report). 825 Victors Way, Ann Arbor, MI 48108: IETF Administrative Support Activity (IASA).

Shue, C., Gupta & M., Davy, M.P. (2008). Packet Forwarding with Source Verification. *Computer Networks:The International Journal of Computer and Telecommunications Networking, 52* (8), 1567-1582.

Wang, H., Jin, C. & Shin, K. G. (2007). Defense against Spoofed IP Traffic using Hop-count filtering. IEEE/ACM *Transactions on Networking, 15* (1), 40-53.

Yaar, A., Perrig, A. & Song, D. (2003). *Pi: A path identification mechanism to defend against DDoS attacks.*

Yaar, A., Perrig, A. & Song, D. (2006). Stackpi: New packet marking and filtering mechanisms for DdoS and IP spoofing defense. *IEEE Journal on Selected Areas in Communications*, *24* (10), 1853-1863.