Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

IP TRACEBACK Scenarios

By Tenali. Naga Mani & Jyosyula. Bala Savitha
CSE Gudlavalleru Engineering College

Abstract - Internet Protocol (IP) trace back is the enabling technology to control Internet crime. In this paper, we present novel and practical IP traceback systems which provide a defense system with the ability to find out the real sources of attacking packets that traverse through the network. IP traceback is to find the origin of an IP packet on the Internet without relying on the source IP address field. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing). Spoof IP packets can be used for different attacks. The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DDoS attack detection.

GJCST-E Classification : C.2.0

Strictly as per the compliance and regulations of:

IP TRACEBACK Scenarios

Tenali. Naga Mani [α] & Jyosyula. Bala Savitha[σ]

Abstract - Internet Protocol (IP) trace back is the enabling technology to control Internet crime. In this paper, we present novel and practical IP traceback systems which provide a defense system with the ability to find out the real sources of attacking packets that traverse through the network. IP traceback is to find the origin of an IP packet on the Internet without relying on the source IP address field. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing). Spoof IP packets can be used for different attacks. The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DDoS attack detection.

I. Introduction

A great amount of effort in recent years has been directed to the network security issues. In this paper, we address the problem of identifying the source of the attack. We define the source of the attack to be a device from which the flow of packets, constituting the attack, was initiated. This device can be a zombie, reflector, or a final link in a stepping stone chain. While identifying the device, from which the attack was initiated, as well as the person(s), behind the attack is an ultimate challenge, we limit the problem of identifying the source of the offending packets, whose addresses can be spoofed. This problem is called the IP traceback problem [1]. IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer [2]. A hacker changes the routing table to point to the spoofed ip address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as trusted users.

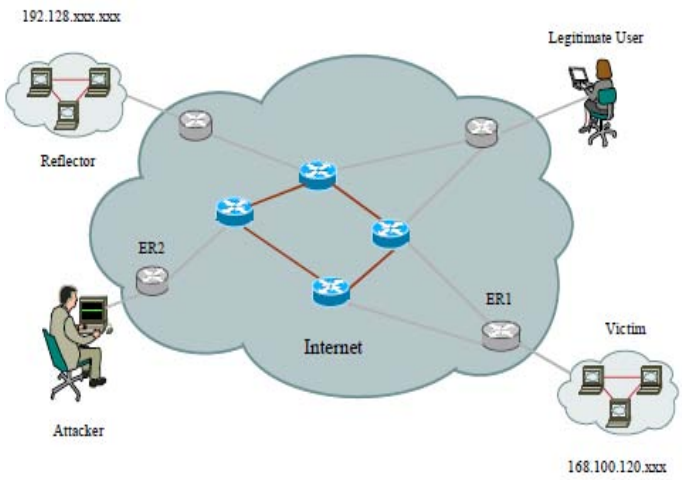

Figure 1 : A Scenario of DOS Attack

Several solutions to this problem have been proposed. They can be divided in two groups. One group of the solutions relies on Fig 1 A Scenario of DOS Attack.

The routers in the network to send their identities to the destinations of certain packets, either encoding this information directly in rarely used bits of the IP header, or by generating a new packet to the same destination. The biggest limitation of this type of solutions is that they are focused only on flood-based (Distributed) Denial of Service [DoS] attacks [3], and cannot handle attacks comprised of a small number of packets. The second type of solutions involves centralized management, and logging of packet information on the network. Solutions of this type introduce a large overhead, and are complex and not scalable.

Author α : Asst. Professor, CSE Gudlavalleru Engineering College Gudlavalleru, Krishna (D.t), A.P. E-mail : tenalinagamani@gmail.com
Author σ : B.Tech (3/4), IT Vijaya Institute of Technology Krishna (D.t), A.P.

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the ip protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for [7] Denial of Service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack). The problem of finding the source of a packet is called the IP traceback problem. IP Traceback [9] is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path(s).

II. Overview

This section provides overview of IP header [2] and the current state of the art approaches to IP traceback and evaluates. While sending data over the internet the IP header contains above details (Fig: 2). Such as type of service, its length, from which source and destination address. Header checksum for error correction and protocol-specifies the type of protocol and set of rules in data exchange.

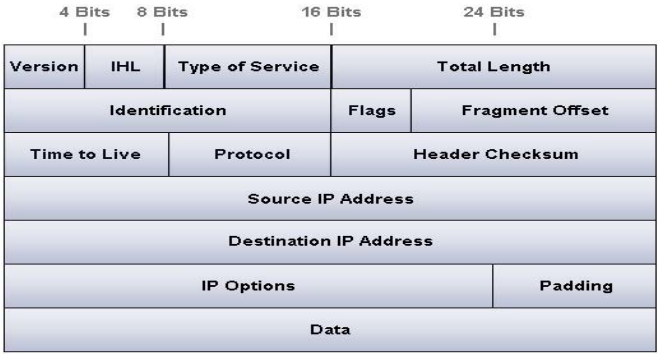

Figure 2 : IP Header

Overview of an ideal traceback system is given below.

- Able to trace the attacker with a single packet.
- Minimal processing overhead during traceback.
- Classification based evaluation.
- No packet transformed through that techniques.
- Limited amount of additional memory requirement at the dedicated server and no additional memory requirement on network
- High level of protection is preferred in a trace back.
- Network overhead based evaluation.
- Router overhead based evaluation.
- Correctly trace back attacks consisting of packets that undergo any number of transformations of any type.
- Producing meaningful traces are limited to the range of deployment of the traceback system.

We are having different traceback schemes exist. Among those FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate according to the load of the participating router by a flexible flow-based marking scheme. Evaluations on both simulation and real system implementation demonstrate that FDPM requires a moderately small number of packets to complete the traceback process; add little additional load to routers and can trace a large number of sources in one traceback process with low false positive rates. The built-in overload prevention mechanism makes this system capable of achieving a satisfactory traceback result even when the router is heavily loaded. The motivation of this traceback system is from DDoS defense. It has been used to not only trace DDoS attacking packets but also enhance filtering attacking traffic. It has a wide array of applications for other security systems.

III. Classification of Traceback Methods

Traceback methods can be broadly categorized [2] as preventive and reactive. Preventive methods take precautionary steps in preventing DoS attacks. A wide range of solutions has been proposed, however, this problem still remains as open one. The reactive methods solutions aim at identifying the source of the attacks. This is very important because attackers spoof their addresses, thus techniques are needed to trace back to the source to the source of the attack. The evaluation is based the above two categorized methods.

a) Preventive Methods

i. *Ingress Filtering*

One way to address the problem of anonymous attacks is to eliminate the ability to forge source addresses. One such approach, frequently called ingress filtering, is to configure routers to block packets that arrive with illegitimate source addresses. This requires a router with sufficient power to examine the source address of every packet and sufficient knowledge to distinguish between legitimate and illegitimate addresses. Consequently ingress filtering is most feasible in customer networks or at the border of Internet Service Providers (ISPs) where address ownership is relatively unambiguous and traffic load is low. As traffic is aggregated from multiple ISPs into transit networks, there is no longer enough information to unambiguously determine if a packet arriving on a

particular interface has a "legal" source address. Moreover, on many deployed router architectures the overhead of ingress filter becomes prohibitive on high-speed links. The principal problem with ingress filtering is that its effectiveness depends on widespread, if not universal, deployment. A secondary problem is that even if ingress filtering were universally deployed at the customer to ISP level, attackers could still forge addresses from the hundreds or thousands of hosts within a valid customer network.

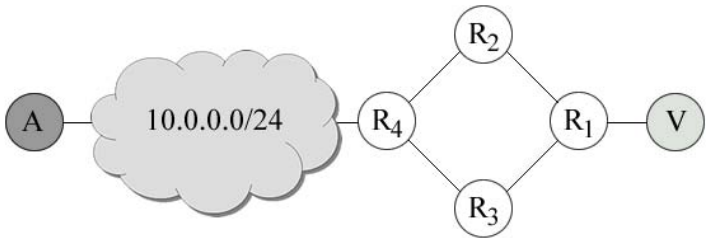

Figure 3 : Ingress Filtering is used at router R4 to prohibit the attacker from using a source IP address residing outside the 10.0.0.0/24 prefix

Ingress filtering restricts the routing of traffic that originates from a downstream network to only well-known and advertised prefixes. Equivalently, a router must drop any packet whose source address does not belong to one of such advertised networks.

Figure 2 depicts a simple network where ingress filtering is used against source address spoofing. For convenience, only IP addresses are used. With ingress filtering, router R4 drops any packet coming from subnet work spoofed source addresses to the victim V.[8] The spoofed source address, however, must reside inside the 10.0.0.0/24 prefix. For instance, the IP address of a neighbor machine could be used as the source address of attack packets. In addition, there is an undesirable dependency between security of end hosts and universal deployment of this technique. Since the filtering directly affects the routing process, inspecting the source address of every packet may also require additional resources from routers. Further, some technologies, such as Mobile IP (Perkins, 2002), legitimately employ spoofed source addresses and could also be affected.

A protection scheme has also been proposed to protect a server from SYN flooding attacks (Belenky and Ansari, 2003). Basically, [7] the scheme keeps track of half-opened TCP connections at a particular server. The tracking is not necessarily implemented on end servers; it can also be implemented on routers and firewalls, for instance. When the number of these connections exceeds a threshold, either new connection requests are blocked, or old half-opened connections are closed in order to make room for new connections. This scheme, however, is specifically designed for this kind of attack and does not provide any information about real perpetrators.

b) Reactive Methods

i. *Link Testing*

Most existing traceback techniques [2] start from the router closest to the victim and interactively test its upstream links until they determine which one is used to carry the attacker's traffic. Ideally, this procedure is repeated recursively on the upstream router until the source is reached. Below describe two varieties of link testing schemes, input debugging and controlled flooding.

a. *Disadvantage*

It consumes huge amount of resources, introduces additional traffic, and possibly causes denial of service when the number of sources needed to be traced increases.

b. *Input Debugging*

Many routers include a feature called input debugging[2],which allows an operator to filter particular packets on some egress port and determine which ingress port they arrived on. This capability is used to implement a trace as follows. First, the victim must recognize that it is being attacked and develop an attack *signature* that describes a common feature contained in all the attack packets. The most obvious problem with the input debugging approach, even with automated tools, is its considerable management overhead. Communicating and coordinating with network operators at multiple ISPs requires the time, attention and commitment of both the victim and the remote personnel many of whom have no direct economic incentive to provide aid.

c. *Controlled Flooding*

Burch and Cheswick have developed a link-testing traceback technique that does not require any support from network operators. We call this technique *controlled flooding [2]* because it tests links by flooding them with large bursts of traffic and observing how this perturbs traffic from the attacker. Using a regenerated

"map" of internet topology, the victim coerces selected hosts along the upstream route into iteratively flooding each incoming link on the router closest to the victim. Since router buffers are shared, packets traveling across the loaded link including any sent by the attacker have an increased probability of being dropped.

c) Drawbacks of Input Debugging

1. A high management overhead.
2. It needs communication and coordination between different ISPs, when the attacking packets traverse different ISPs networks.
3. This scheme works only for ongoing attacks. The last but not the least, it requires network administrators to have the appropriate technical skills and capabilities.

i. *Logging*

An approach suggested is to log packets at key routers and then use data mining techniques[9] to determine the path that the packets traversed. This scheme has the useful property that it can trace an attack long after the attack has completed. However, it also has obvious drawbacks, including potentially enormous resource requirements and a large scale interprovider database integration problem. We are unaware of any commercial organizations using a fully operational traceback approach based on logging.

ii. *ICMP Traceback*

Internet Control Message Protocol (ICMP) in need of trace out full path of the attacks. This approach was originally introduced by Bellovin. The principle idea in these schemes is for every router to generate an ICMP traceback message or iTrace directed to the same destination as the selected packet. The iTrace message itself consists of the next and previous hop information and a time stamp As packets travel through the network, they gather and store information about the routers they traverse.

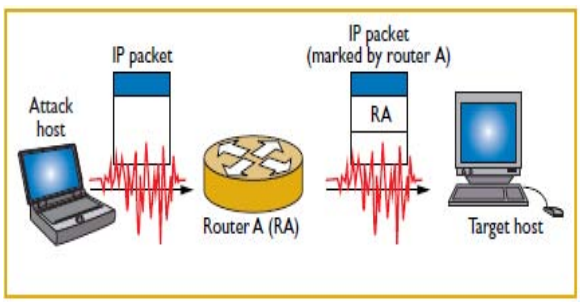

Figure 4 : Packet Marking

A router creates an ICMP traceback message, which contains part of a traversing IP packet, and sends the message to the packet's destination. We can identify the traversed router by looking for the corresponding ICMP traceback message and checking its source IP address. Because creating an ICMP traceback message for every packet increases network traffic, however, each router creates ICMP traceback messages for the packets it forwards .If an attacker sends many packets the target network can collect enough ICMP traceback messages to identify its attack path.

iii. *Packet Marking Algorithm*

In Packet Marking Algorithm [5] schemes, each router in addition to forwarding a packet also inserts a mark in the packet. This mark is a unique identifier corresponding to this particular router.

As a result the victim can determine all the intermediate hops for each packet by observing the inserted marks. There are two variants to this marking scheme. First is the Deterministic Packet Marking [5] (DPM) scheme in which each router marks all the packets passing through it with its unique identifier? This scheme is thus similar to the IP record-route option. This makes the reconstruction of the attack path at the victim trivial. But the downside to this scheme is that routers are slowed down as they have to perform additional functionality. An attacker who controls a trusted router can forge any path up to that router unless some further authentication scheme is used. A router that trusts data from an attacker effectively allows that attacker to act like a compromised router. Authentication methods could be used, but these add significant cost in the form of processing time and space in the marked packets. A downside of this scheme is that some packets will not be overwritten by any of the routers. The attacker can therefore write bogus information in all the packets knowing that some of these packets will get through and confuse the victim. This method also does not work well for DoS attacks that can work without a lot of packets as it requires a large number of packets to converge. The second instances is probabilistic packet marking[10] (PPM), DoS attacks can be prevented if the spoofed source IP address is traced back to its origin which allows assigning penalties to the offending party or isolating the compromised hosts and domains from the rest of the network.

Recently IP traceback mechanisms based on probabilistic packet marking have been proposed for achieving traceback of DoS attacks. In this paper, we show that probabilistic packet marking of interest due to its efficiency and implement ability vis-à-vis deterministic packet marking and logging or messaging based schemes suffers under spoofing of the marking field in the IP header by the attacker which can impede traceback by the victim. Attacks on PPM: Attacks involving spoofed traceback data are described in. In general the two major problems in PPM reliability are the probabilistic nature of the algorithm causes some packets not to be marked by cooperating routers and these retain whatever marks are given them by the senders. Attackers can simply mark their original packets to intentionally mislead the traceback mechanism. In DPM routers mark all forwarded packets

with link identifying data. With PPM, multiple routers on the paths overwrite the same data, and each packet identifies at most one link. With DPM, each co-operating router adds link identifying data to the packet and each packet ends up with data that identifies all of the links (under universal co-operation) that it traversed.

a. *Disadvantages of Packet Marking*

1. Mark Length: It cannot adjust the length of marking field according to the network protocols deployed.
2. Marking Rate is not flexible according to the load of the participating router.
3. Number of Packets required is comparatively more.
4. False Positive rate is large.
5. Tracing Capability is less.
6. The path reconstruction process requires high computational work, especially when there are many sources. For example, a 25-source path reconstruction will take days, and thousands of false positives could happen.
7. When there are a large number of attack sources, the possible rebuilt path branches are actually useless to the victim because of the high false positives.

iv. *FDPM Traceback*

Flexible Deterministic Packet Marking [6] (FDPM) is the optimized version of DPM. This scheme provide more flexible features to trace the IP packets and can obtain better tracing capabilities over other previous IP traceback mechanisms, such as Link testing, logging, ICMP traceback, probability packet marking (PPM) and Deterministic packet marking (DPM).In FDPM schemes, the Types of Services (ToS) fields will be used to store the mark under some circumferences. The two fields in the IP header are exploited, one is fragment ID and other is Reversed flag. An identifying value is assigned to the ID field by the sender to aid in assembling the fragments of a datagram. Given that less than0.25%of all internet traffic is fragments, this field can be safely overloaded without causing serious compatibility problems. FDPM reconstruction process includes two steps: mark recognition and address recovery. Compared to DPM [5], the reconstruction process is simpler and more flexible. When each packet that is used to reconstruct the source IP address arrives at the victim, it is put into a cache, because in some cases the processing speed is lower than the arrival speed of the incoming packets.

The FDPM [6] scheme utilizes various bits (called marks) in the IP header. The mark has flexible lengths depending on the network protocols used, which is called flexible mark length strategy. When an IP packet enters the protected network, it is marked by the interface close to the source of the packet on an edge ingress router.

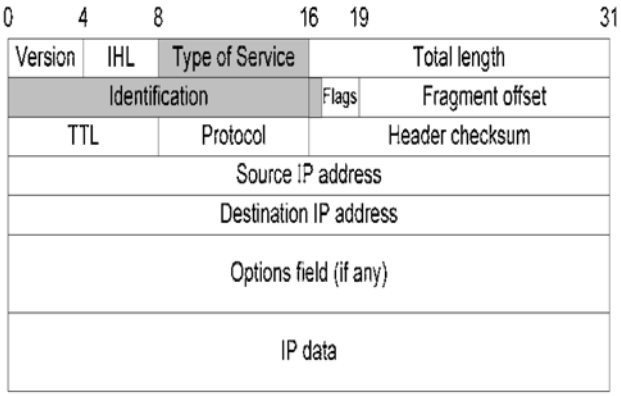

Figure 5 : IP (darkened) headers utilized in FDPM

The source IP addresses are stored in the marking fields. The mark will not be overwritten by intermediate routers when the packet traverses the network. At any point within the network, e.g., the victim host, the source IP addresses can be reconstructed when required. Processing packets consume resources such as memory and CPU time of a participating router. Therefore, it is possible for a router to be overloaded when there are a large number of arrival packets waiting for FDPM to mark them.

The flow-based marking scheme is proposed to solve the overload problem. When the load of a router exceeds a threshold, the router will discern the most possible attacking packets from other packets then selectively mark these packets. The aim is to alleviate the load of the router while still maintaining the marking function.

a. *Advantages*

1. Easy to find out packet loss and Duplicate packets.
2. Reduces the network traffic.
3. Bandwidth consumption is less.
4. Flexible mark length: The length of marking field can be adjusted according to the network protocols deployed.
5. Flexible mark rate: The marking rate can be changed adaptively according to the load of the participating router.
6. Low false Positive rate.
7. Number of packets required is comparatively less.
8. Better Tracing Capability.
9. It has Different probabilities that a router marks the attack packets.

v. *TBPM Method*

Topology [9] aware single packet IP traceback system is namely TOPO. It is based on the bloom filter which utilizes router's local topology information, i.e., its immediate predecessor information, to traceback. TOPO can significantly reduce the number and scope of unnecessary queries and thus, significantly decrease the false attributions to innocent nodes. The main goals of TOPO as follows:

1. To design a single packet IP traceback system, this has fewer unnecessary query messages and fewer false attributions to innocent nodes.
2. To design a single packet IP traceback system this needs not to be fully deployed in the entire network.
3. To design a mechanism which helps achieve the best performance of Bloom filters by adaptively adjust using parameter.

Topology Based Packet Marking (TBPM) has been a new approach in Anti-IP spoofing techniques.

TBPM builds on the strengths of the packet marking principal; however it focuses not merely on the source, but also the path traversed by a datagram. We have pointed out how a route discovery method can be more effective, especially during DoS attacks where edge routers that mark packets may themselves be unavailable as a result of the attack. Embedded topological information may enable DoS attacks to be prevented even by intermediate routers. TBPM also enables the source to be identified using a single marked packet; unlike previous techniques that require multiple packets. TBPM techniques are compatible with both IPv4 and IPv6; unlike present packet marking techniques that cannot be effectively implemented in IPv6 networks.

IV. Technologies for Preventing Network Attacks

Current technologies for protecting networks against attacks focus on access control and attack detection [2]. Although some methods can find the attacker's identity, they are unsuccessful when the attacker's true IP address is hidden or unknown.

a) Firewalls

Firewalls are widely used to protect networks against attacks, especially those coming from the Internet. Usually, firewalls control access based on source IP address, destination IP address, protocol type, source port number, and destination port number. For example, we can configure a firewall to deny any access to a WWW server except for WWW access using HTTP (destination port number 80). If an attacker attempts to exploit the WWW server using HTTP, however, the firewall cannot prevent it.

b) Intrusion Detection

An intrusion detection system (IDS) detects network attacks to a computer system. One major method currently implemented in IDS products is misuse detection. In this method, the IDS compare the attack signatures, which are features of known attacks, with the contents of packets on the network or log data on the host computer. When the packet content or log data matches an attack signature, the system recognizes that an attack has occurred. IDSs still pose accuracy problems for site managers, however. In practice, IDSs detect possible attacks, which site managers must examine to determine whether it is a real attack.

c) Intrusion Source Identification

Using IDSs, we can detect certain attacks and find the attack packets' source IP addresses. Because the IP address is not enough to identify the attack source, however, we typically run a DNS inverse query to check the fully qualified domain name (FQDN),or look up the database in a WHOIS server to find the source identity (for example, organization name and e-mail address). If the attack's purpose is penetration or reconnaissance, most attackers will hardly disguise the source IP address because they must receive a response from the target.

An attacker who aims for denial of service (DoS), however, does not need to receive packets from the target and can therefore forge its source IP address. Ingress filtering deals with forged addresses.1 in this method, a router compares an incoming packet's source IP address with a router's routing table and discards packets with inconsistent source addresses as having been forged. This method is effective for many spoofed DoS attacks, but it fails if an attacker changes its source IP address to one that belongs to the same network as the attacker's host.

V. Limitation and Open Issues

IP traceback has several limitations [1], such as the problem with tracing beyond corporate firewalls. To accomplish IP traceback, we need to reach the host where the attack originated. It is difficult, however, to trace packets through firewalls into corporate intranets the last- traced IP address might be the firewall's address. Knowing the IP address of the organization's network entry point, however, allows us to obtain information about the organization where the attacker's host is located, such as the organization's name and the network administrator's e-mail address. If we can identify the organization from which the attack originated, the organization can often identify the user who launched the attack.

Another limitation relates to the deployment of traceback systems. Most traceback techniques require altering the network, including adding router functions and changing packets. To promote traceback approaches, we need to remove any drawbacks to implementing them.

Moreover, even if IP traceback reveals an attack's source, the source itself might have been used as a stepping-stone in the attack. IP traceback methods cannot identify the ultimate source behind the stepping-stone; however, techniques to trace attacks exploiting stepping-stones are under study. Some operational issues must also be solved before IP traceback can be widely deployed. To trace an attack packet through

different networks, for example, there must be a common policy for traceback. We also need guidelines for dealing with traceback results to avoid infringing on privacy. Furthermore, we need to consider how to use information about an attack source identified by IP traceback.

VI. Conclusion

One conclusion we can draw from this is that unless IP trace back measures are deployed all over the Internet, they are only effective for controlled networks than for the Internet. Today we can find many tools for doing DoS attacks. DoS attacks have become very popular. Hence we need to design proper mechanisms to protect systems from such attacks. Mechanisms has been developed and deployed to prevent such attacks. But DDoS is still a problem as it is difficult to trace DDoS attackers and its effect is too bad. We need to start development towards defending DDoS. Some schemes are present which very well defends such attacks, but without the cooperation of ISPs it will be difficult to deploy any scheme. Though RFC asks to deploy ingress filtering, still very less number of ISPs have deployed that. Mechanisms like hash based traceback leads to many management issues, which in current scenario doesn't seem to be working. Mechanisms are there which talks about single packet traceback, but there are lots of overheads for such methods.

References Références Referencias

1. http://en.wikipedia.org/wiki/IP_traceback
2. IP Traceback: A New Denial-of-Service And different IP hacking approaches from google search engine.
3. http://cseweb.ucsd.edu/~savage/papers/Ton01.pdf: "Different :IPtraceback approaches"
4. G. Jin and J. Yang, "Deterministic Packet Marking Based on Redundant Decomposition for IP Traceback," IEEE Comm. Letters,vol. 10, no. 3, pp. 204-206, 2006.
5. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164, 2003.
6. Y. Xiang, W. Zhou, and J. Rough, "Trace IP Packets by Flexible Deterministic Packet Marking (FDPM)," Proc. IEEE Int'l Workshop IP Operations and Management (IPOM '04), pp. 246-252, 2004.
7. H. Farhat, "Protecting TCP Services from Denial of ServiceAttacks," Proc. ACM SIGCOMM Workshop Large-Scale AttackDefense (LSAD '06).
8. H. Aljifri, "IP Traceback : A New Denial-of-Service Deterrent,"IEEE Security and Privacy, vol. 1, no. 3, pp. 24-31, 2003.
9. Study on Flexible Deterministic Packet Marking An IP Traceback System - 1.IJAEST-Vol-No-9-Issue-No-1-A-Study-on-Flexible-Deterministic-Packet-Marketing-An-IP-Traceback-System-001-007.pdf.
10. M. Adler, "Trade-Offs in Probabilistic Packet Marking for IP Traceback," J. ACM, vol. 52, no. 2, pp. 217-244, 2005.

This page is intentionally left blank