**A RISK CLASSIFICATION BASED APPROACH FOR MALWARE IP-SPOOFING ATTACK DETECTION**

**ABSTRACT**

IP spoofing remains a popular method to launch Distributed Denial of Service (DDOS) attacks through Malware. 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 "Border Gateway Protocol (BGP)" route 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 project we propose an Risk Classification Credible BGP (CBGP) based on IDPF approach to 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 CBGP assigns credibility scores for "Autonomous Systems (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.

**1. INTRODUCTION**

Every transfer of data across the internet involves capturing of IP address. A simple Google search involves tracking the IP of Google server back to the source system’s IP. Since IP capture is accomplished in each and every point of transfer or exchange of data across the network, IP capture is easy to do and this can be added as a security feature to e-learning content retrieval system.

This e-learning system captures the IP address of the registered user. When a user tries to retrieve the contents from the e-learning environment other than logging in from other IP address, the content delivery is prohibited. But there are chances that this IP captured from the registered users may be spoofed by unauthenticated users to gain access to the content of the e-learning system. Also it is better to improve the document based search techniques we need to incorporate class hierarchy methods.

The advanced AES algorithm coding formula can be embedded to produce secured transaction in the distributed system by means of dynamic key generation for various information sets. To ensure the learning to be the lifelong process the system can be designed with pedagogical virtual agents who have the aesthetic value.

IP Spoofing can be achieved by intruding the end systems i.e. the source and the destination systems. The intruder captures the IP of the source machine and assigns its IP on the packets being sent to the destination machine, thus making the destination machine to believe the intruder to be the legitimate source machine that had sent the request.

The main aim of the intruder here is to establish a duplicate connection between itself and the destination machine to steal and gain access to access restricted data. Normally, when there is a communication between two machines, let us say machine SRC and machine DST where SRC is the source machine and DST is the destination machine. The exchange of data is carried out as shown in Figure 1, Figure 2 and Figure 3.

This type of IP spoofing is done to impersonate and steal and gain access to data whereas when the aim is to do a DOS attack the Scenario will be as shown in Figure 4. The attacker spoofs the IP of the target and broadcasts ICMP Echo Requests to machines in a network. When all the machines respond to the target with ICMP Echo reply the victim or the server is brought down and faces a DOS attack. This attack is termed as Smurf attack.



Figure 1. Common communication method.



Figure 2. Normal communication between two machines.



Figure 3. IP spoofing.



Figure 4. DOS attack using IP spoofing.



Figure 5. MITM attack.

IP Spoofing may be done with two intents impersonation and for performing a DOS attack. DOS attacks are done to bring down a server by flooding the server with TCP/SYN packets of ICMP Requests for which the server will not be able to respond. The impersonation attack is done to gain access or to capture traffic between two nodes on a network. The first type of attack is the one that has to be focused in this Learning and Content Management Systems since the impersonation may lead to piracy of the contents in the system.

Network level attacks include IP spoofing. Network level implementation device is the router and when the router is configured with proper Intrusion Prevention System and Intrusion Detection System impersonation or a DOS attack can be mitigated. Ingress Filtering is one technique that can be used to mitigate IP spoofing attacks. This method proposes filtering of the data received at the destination where the data packets from the specified source are checked for its integrity and authenticity.

Tracing back to the source IP will yield better results in mitigating IP spoofing attacks. Trace back is a method that traces the IP from which the data packets are received at the destination. This technique must be added to the router configuration which will dissipate packets from illegitimate source IPs.

**2. SYSTEM STUDY**

System analysis will be performed to determine if it is flexible to design information based on policies and plans of organization and on user requirements and to eliminate the weakness of present system. This chapter discusses the existing system, proposed system and highlights of the system requirements.

**2.1 EXISTING SYSTEM**

Routing of a packet to its origination is possible which would help in detection of a IP spoofed packet entering the network. The process of disallowing the spoofed packets from getting into the network is called as "Egress Filtering". This method filters the outbound traffic entering the network. The process of disallowing spoofed packets from getting out of our network is called as ingress filtering. This method filters the inbound traffic raising from the Internal IP to the NAT table and then to the External IP and being sent to the public network to reach the destination. When deciding on the best fitness route, there are some considerations to make, including a short route, the amount of energy, and the quantity of data traffic even if a data packet is dropped randomly.

**DISADVANTAGES:**

* The delay and routing overhead are comparatively high because the node's clan needs to be updated frequently which rises the routing overhead and causes delay.
* However, this method did not consider the reliability of the routes in the sense of data collision rate and link stability.

**2.2 PROPOSED SYSTEM**

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. This is impossible with the current BGP-based Internet routing infrastructure. The current Internet topology consists of more than 35,000 network domains or ASs, each of which is a logical collection of networks with common administrative control. Each AS communicates with its neighbors using the BGP, the de-facto inter-domain routing protocol, to exchange network layer information reachability about its own networks and others that it can reach. BGP is a policy-based routing protocol in that both the selection and the propagation of the best route to reach a destination at an AS are guided by some locally defined routing policies. 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 is an open challenge in the current Internet routing regime. The proposed Risk Classification Credible BGP (CBGP) based on 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. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. When a node receives a packet from an incoming interface, it checks if the source IP address has been advertised through this interface. The packet is discarded if the check is negative. A key feature of the scheme is that it does not require global routing information.

**ADVANTAGES:**

* The simulation results showed that, even with partial deployment on the Internet, IDPFs can significantly limit the malwasre spoofing capability of attackers.
* Moreover, they also help localize the actual origin of an attack packet to be within a small number of candidate networks.
* In addition, IDPFs also provide adequate local incentives for network operators to deploy them.

**3. SYSTEM SPECIFICATION**

**3.1 HARDWARE SPECIFICATION**

Processor : i3 and above

RAM : 2 GB and above

HDD : 500GB and Above

**3.2 SOFTWARE SPECIFICATION**

Operating System : Windows XP/8/10

Programming Language : Java

IDE : My Eclipse 6.0

Back End : Buffer Storage

**MODULES DESCRIPTION:**

**(i) Credible BGP**

CBGP calls for a modification to the standard BGP route selection algorithm such that it takes into account validity state of routing updates. We define the validity state factor as the minimum of two independent scores, route origination validation score and update AS path validation score. 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.

**(ii) BGP Decision Process**

The BGP decision process will then be modified to check the validity state of each routing update when comparing two routing updates for routing selection purposes. The validity state check must be performed before any of other prior to any of the steps defined in the decision process. The route with the highest validity state will always be preferred over other routes. In all other respects, the BGP decision process remains unchanged.