International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Detection and Prevention of IP Spoofing Attack

A. Dhilipan[1], Ms. Sarika Jain[2], Dr. S. Geetha[3]

[1]M.Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2]Center of Excellence in Digital Forensics, Chennai 600 089, Tamilnadu, India

[3]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

Abstract

In Computer Networking, IP address Spoofing or IP Spoofing is the creation of Internet Protocol packets with a false source IP address, for the purpose of impersonating another computing system. DNS (Domain Name System) amplification attack is a popular form of (Distributed Denial of Service) DDoS attacks that relies on the use of Open Resolver (publically accessible DNS servers) to overwhelm the victim (i.e., target of DNS amplification attack) with amplified DNS traffic. This attack is based on a recursive function of DNS servers. This attack is based on a recursive function of DNS servers.

Keywords: DNS; DDoS attacks.

1. Introduction

DNS intensification assault is a famous type of DDoS assaults that depends on the utilization of Open Resolver (freely open DNS servers) to overpower the person in question (i.e., focus of DNS enhancement assault) with enhanced DNS traffic. This assault depends on a recursive capability of DNS servers. Typically, the DNS server acknowledges and answer's goal demands from anybody without confirming its character. Consequently, aggressors can take advantage of recursive capabilities to intensify the assault by parodying the casualty's IP address. The mock questions (i.e., DNS demands) sent by the assailant are of type ANY; they incorporate all known data about a DNS zone in a solitary solicitation. The enhancement effect of this assault comes from the way that little questions can produce monstrous measures of UDP bundles accordingly. This class of assault can be isolated in two sorts: (a) enhancement with rehashed DNS demands that have a similar substance; and (b) intensification with fluctuated DNS demands that have various items. The inquiry can be of type ANY that demands all records for a specific space or various spaces. The size of the reaction might be enormous to deliver an elevated degree of enhancement. The intensification proportion, of a variable up to 4670, is determined as the proportion between the reaction size and the solicitation size. As per a new report, there are around 7.5 million outside DNS servers in the Web; over 75% of these servers permit recursive name administration to people in general. This can cause huge inadvertent blow-back on the person in question, assuming aggressors utilize numerous recursive servers to enhance and produce the assault. This assault is considered as the biggest ever DDoS assault, surpassing a pace of 1 Tbit/s. Such occurrences hurt Network access suppliers (ISPs) and cost great many dollars of lost incomes for endeavours.

2. Literature Survey

Mohammed Moin Mulla et.al, Distributed Denial of Service Attacks (DDoS) are most widely used cyberattacks. Thus, design of DDoS detection mechanisms has attracted attention of researchers. Design of these mechanisms involves building statistical and machine learning models. Most of the work in design of mechanisms is focussed on improving the accuracy of the model. However, due to large volume of network traffic, scalability and performance of these techniques is an important research issue. In this work, we use Apache Spark framework for detection of DDoS attacks. We use NSL-KDD Cup as a benchmark dataset for experimental analysis. The results reveal that random forest performs better than decision trees and distributed processing improves the performance in terms of pre-processing and training time.

Sungwoong Yeom et.al, as the trouble of Distributed Denial- of- Service attacks exploiting IoT bias has spread, source- side Denial- of- Service attack discovery styles are being studied in order to snappily descry attacks and find their locales. also, to alleviate the limitation of original view of source- side discovery, a cooperative attack discovery fashion is needed to partake discovery results on each source- side network. In this paper, a new cooperative source- side DDoS attack discovery system is proposed for detecting DDoS attacks on multiple networks more rightly, by considering the detecting performance on different time zone. The results of individual attack discovery on each network are ladened grounded on discovery rate and false positive rate corresponding to the time zone of each network. By gathering the weighted discovery results, the proposed system determines whether a DDoS attack happens. Through expansive evaluation with real network business data, it's verified that the proposed system reduces false positive rate by 35 while maintaining high discovery rate.

Faisal Hussain et.al, the botnet attack is a multi-stage and the most prevalent cyber-attack in the Internet of Things (IoT) environment that initiates with scanning activity and ends at the distributed denial of service (DDoS) attack. The existing studies mostly focus on detecting botnet attacks after the IoT devices get compromised, and start performing the DDoS attack. Similarly, the performance of most of the existing machine learning based botnet detection models is limited to a specific dataset on which they are trained. As a consequence, these solutions do not perform well on other datasets due to the diversity of attack patterns. Therefore, in this work, we first produce a generic scanning and DDoS attack dataset by generating 33 types of scans and 60 types of DDoS attacks. In addition, we partially integrated the scan and DDoS attack samples from three publicly-available datasets for maximum attack coverage to better train the machine learning algorithms. Afterwards, we propose a two-fold machine learning approach to prevent and detect IoT botnet attacks. In the first fold, we trained a state-of-the-art deep learning model, i.e., ResNet-18 to detect the scanning activity in the premature attack stage to prevent IoT botnet attacks. While, in the second fold, we trained another ResNet-18 model for DDoS attack identification to detect IoT botnet attacks. Overall, the proposed two-fold approach manifests 98.89% accuracy, 99.01% precision, 98.74% recall, and 98.87% f1-score to prevent and detect IoT botnet attacks. To demonstrate the effectiveness of the proposed two-fold approach, we trained three other ResNet-18 models over three different datasets for detecting scan and DDoS attacks and compared their performance with the proposed two-fold approach. The experimental results prove that the proposed two-fold approach can efficiently prevent and detect botnet attacks as compared to other trained models.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

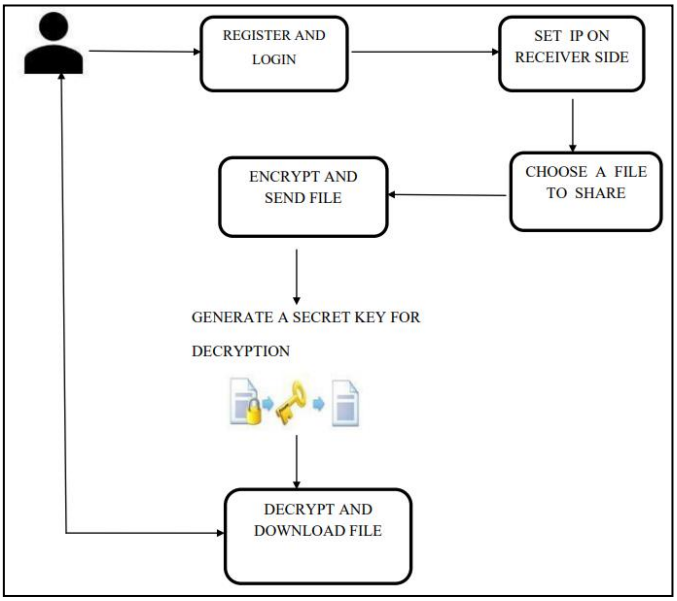
3. Existing System

The being system requires the global routing information to defend IP burlesquing effectively. The being SDMN control channel is to TCP DoS and reset attacks. We observed that it wasn't possible to establish connections with the regulator during TCP SYN DoS attacks and during the TCP reset attack it wasn't possible to modernize the inflow tables.

4. Proposing System

The proposed novel proactive and stateful scheme (PAS) to perform one-to-one mapping between DNS requests and DNS responses. And a flow statistics collection scheme (FSC) to gather the features of flows in an efficient way using sFlow protocol. We introduce an entropy calculation scheme (ECS) to measure the disorder/randomness of network traffic. We propose a Network based Filtering scheme (BNF) to classify, based on entropy values, illegitimate DNS requests. We propose a DNS Mitigation scheme (DM) to effectively mitigate illegitimate DNS requests. The architecture consists of an SDN Open flow switch (OFS) connecting network servers to the Internet through a core network or directly via a gateway. By taking advantage of SDN, in this paper, we propose an SDN based Integrated IP Source Address Validation Architecture (ISAVA) which can cover both intra- and inter-domain areas and effectively lower SDN devices deployment cost, while achieve desirable control granularities in the meantime.

5. Architecture Diagram



5.1 Architecture Diagram

6. List of Phases

There are 4 phases

- Sender
- Admin
- Router
- Receiver

6.1 Sender

The Owner associated items are viewed by the users and the results can be summed up from the users, because they are using this system and according to their response the association technique works.

Login

Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site.

Registration

A registered stoner is a stoner of a website program or other system who has preliminarily registered. Registered druggies typically give some kind of credentials (similar as a username ore-mail address, and a word) to the system in order to prove their identity this is known as LOGGING IN. Systems intended for use by the general public frequently allow any stoner to register simply by opting a register or subscribe up function and furnishing these credentials for the first time. Registered druggies may be granted boons beyond those granted to unrecorded druggies.

Upload and Share File

In this module User can upload and share data to any other users.
View Shared File:
Receiver can view file details who shared by them.
Encrypt the File:
Encrypt the file which has to be sent to the receiver through IP.

6.2 Admin

This part is the controller of the system. He can view the whole summary of the system if the system consists of many organizations. Also, he can analyze the present trend in the public.

Login

Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site.

View User Details

In this module admin can view all details of users.

6.3 Router

Login

Logging in is usually used to enter a specific page, which trespassers cannot see. Once the router is logged in, the login token may be used to track what actions the router has taken while connected to the site.

IP Source Address Filtering

Depending on the acting positions, filtering solutions can be divided into three types: ingress-, egress- and router-based filtering, which checks packet legitimacy in router's ingress ports, egress ports and internal modules, respectively. For instance, the unicast Reverse Path Forwarding (uRPF) is a deployable ingress filtering solution, 19 which was advocated by Cisco and applied to its products. When uRPF function is enabled, for every packet, router's ingress port first looks up its Forwarding Information Base (FIB) with packet's IP source address, so that it can verify the packet's legality based on whether the forwarding port matches the current ingress port or not. However, uRPF is proprietary mechanism and it is hard to cope with the situations when both the victim and the attacker are in the same direction, routing asymmetry and etc.

IP Source Address Encryption

In order to authenticate communication correspondents, some researchers give their solutions from the angle of replacing the IP source address with the encrypted one. For example, Cryptographically Generated Addresses (CGA) and Accountable Internet Protocol (AIP) encrypt IP source address with the asymmetric key cryptography so that keys sharing both ends can verify each other. But such designs need extra secure key agreement protocols because key generation and public-key distribution are accomplished by individual hosts without Certificate Authority (CA), which is non-suitable for large-scale networks. To address this issue, True IP takes IP source address as the public key and utilizes the Identity Based Cryptography (IBC) to produce the private key, so that correspondents can verify the authenticity of each other directly without public-key acquirements. However, it is uneasy to revoke IBC keys since all keys need to be regenerated if one private key is compromised.

6.4 Receiver

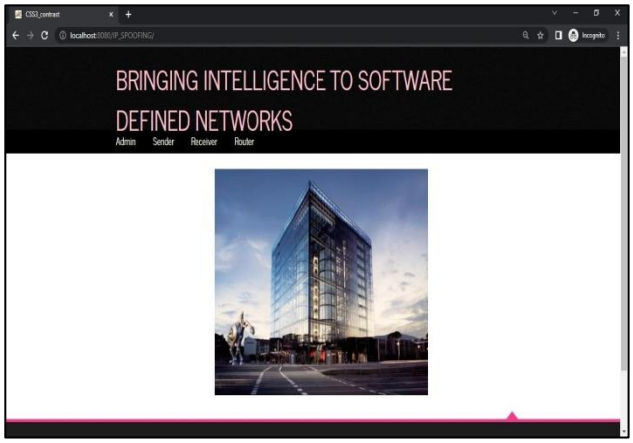
Login

Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site.

Access the File with Public Key
To access the File the receiver should have the public key from the sender.
Decrypt the File
Decrypt the encrypted file which has been sent by the sender.

7. Screenshots

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

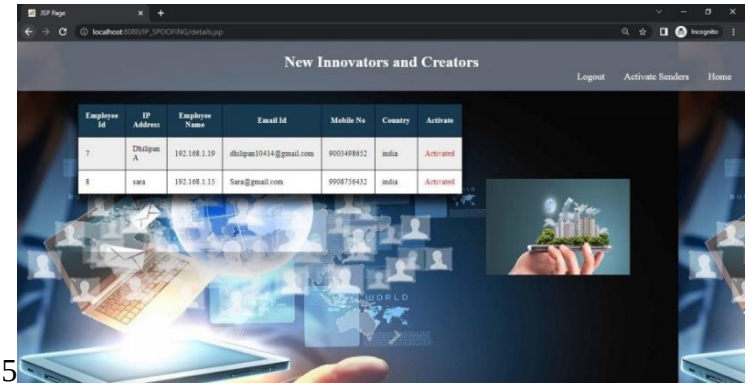


Home Page

Signup Page

Admin Login Page

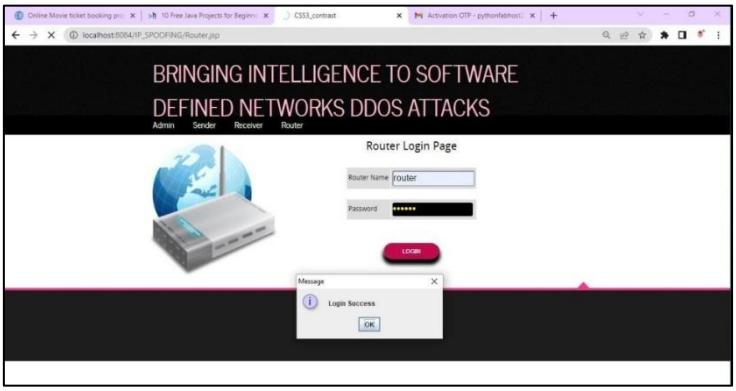
International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



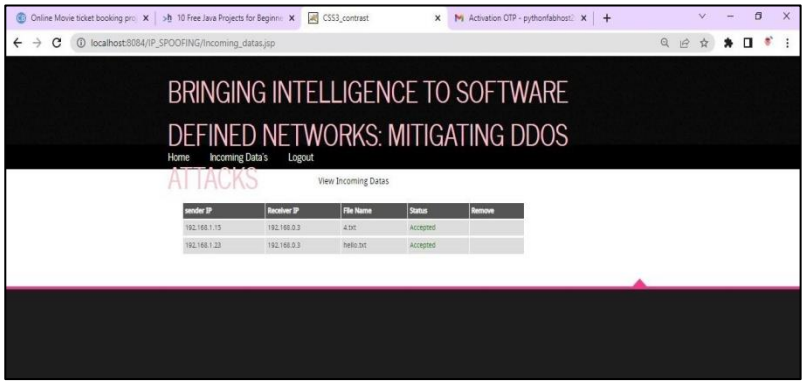
5

Sender Login Page

Admin Activation Page

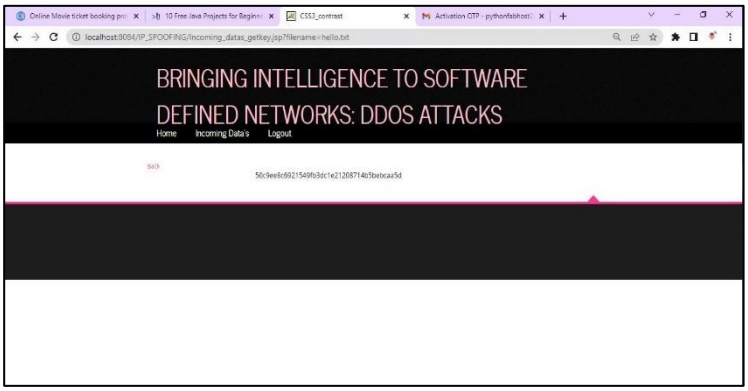


Router Login Page

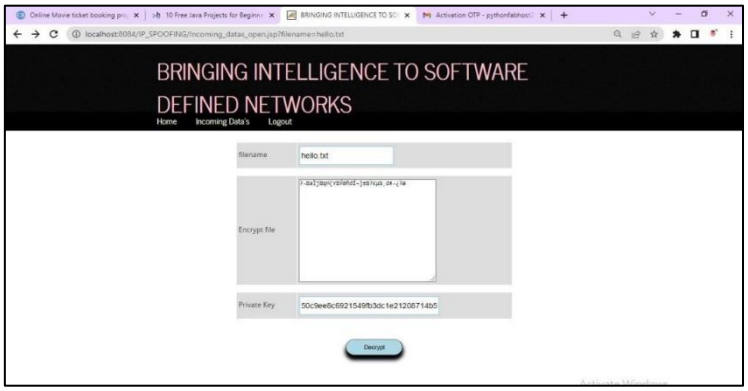


International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

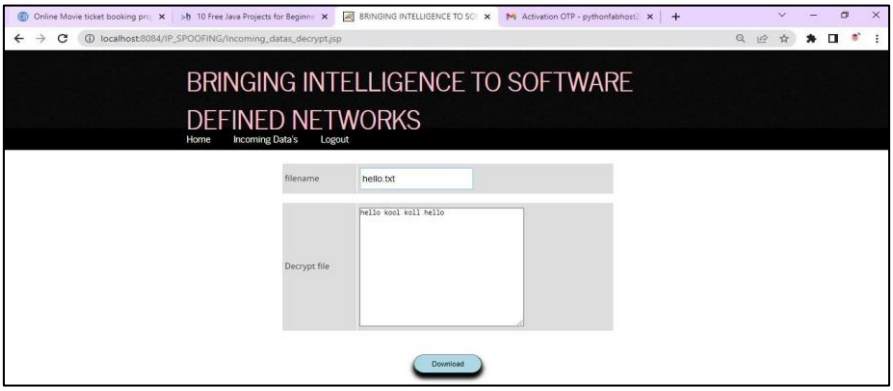
Router Incoming Data



Decrypting the File



Decrypted File



8. Conclusions

SDN is an emerging technology that brings numerous benefits by decoupling the control plane from data plane. On one hand, the separation of the control plane from the data plane allows for more control over the network and brings new capabilities to deal with large forms of DDoS attacks. On the other hand, this separation introduces new challenges regarding the security of the control plane. This paper aims to deal with DNS amplification attack while maintaining the SDN secure (i.e., protecting the resources of data plane (i.e., Ternary Content Addressable Memory (TCAM) of switches). For this aim, the proposed PAS, a proactive and stateful scheme that performs a one-to-one mapping between DNS request and DNS response in order to: (1) protect the victim from DNS amplification attack; and (2) protect the

resources of the SDN controller. Then, the proposed machine learning DDoS detection module that consists of FSC, ECS and BNF in order to detect illegitimate DNS requests and protect TCAM of switches. Finally, DM is designed to mitigate illegitimate DNS requests. In our simulations, set a fixed idle and hard timeouts of flow rules. For large values, flow rules stay in OF table for a long time which can exhaust TCAM of switches, while too small values, may lead to the dropping of legitimate DNS responses.

References

[1] C. Rossow, ―Amplification hell: Revisiting network protocols for ddos abuse, ‖ in In Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS, 2014.

[2] Dns expertise. ‖ Accessed: June. 1, 2019. [Online]. Available: http://dns.measurementfactory.com/surveys/sum1.html

[3] S. Sharwood, ―Github wobbles under ddos attack. ‖ Accessed: June. 1, 2019. [Online]. Available: https://www.theregister.co.uk/2015/08/26/ github_wobbles_under_ddos_attack

[4] B. Schneier, ―Lessons from the dyn ddos attack. ‖ Accessed: June. 1, 2019. [Online]. Available: https://www.schneier.com/blog/archives/ 2016/11/lessons_from_th_5.html

[5] S. Scott-Hayward, S. Natarajan, and S. Sezer, ―A survey of security in software defined networks, ‖ IEEE Communications Surveys Tutorials, vol. 18, no. 1, pp. 623–654, First quarter 2016.