Denial of Service (DoS) attacks is a kind of attacks against computers connected to the Internet. The goal of DoS attacks is to keep away authorized users from accessing resources. The infected computers may crash or disconnect from the Internet. The distributed denial of service (DDoS) attack is a continuous critical threat that has caused severe damage to servers and will cause even greater intimidation to the development of new Internet services. In the present scenario the mitigation of these attacks has most importance. There are a number of mitigation techniques have been proposed by various researchers. A Web Referral Architecture for Privileged Services (WRAPS) proposed by the authors [8], that can mitigate the DDoS attack that plague website today. It allows a legitimate client to obtain a privileged URL by a referral hyperlink, from a website trusted by the target website. There are several limitations are present in this architecture. WRAPS support only clients that use fixed IP address, instead of as domain names it encodes privileged URLs as IP addresses. If the users want privileged services, then they must access the target site through privileged URL. That means the domain name of server not resolved via DNS and the users must save their privileged URL from the server when it is updated at the end of a privileged period, thus WRAPS not transparent to users.
Mitigation of Distributed Denial of Service (DDoS) Threats

References

- M. Nagaratna, Dr. V. Kamakshi Prasad and S. Tanuz Kumar, “Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking based Detection And Filtering (EMDAF)”. International Conference on Advances in Recent Technologies in Communication and Computing, IEEE 2009.

Index Terms

Computer Science Security

Keywords
Distributed Denial of Service Denial of Service