Abstract

With the increase in web-based transactions and communications, Distributed Denial of Service (DDoS) attack is becoming a very critical threat to the web. Also the popularity of application services offered by Internet has grown a lot in recent years. Countering DDoS attacks is becoming ever more challenging with the vast resources and techniques increasingly available to attackers. Derived from the low layers, new application-layer-based DDoS attacks utilizing legitimate HTTP requests to overwhelm victim resources are more undetectable. DDoS attacks are typically carried out at the network layer. However, application layer DDoS attacks can be more effective than the traditional network layer attacks. Many methods were designed in previous literatures to protect systems from IP and TCP layers DDoS attacks instead of the application layer. However, they will not work well any more when encountering with application layer DDoS attack. Most of the network layer DDoS attacks are flooding attack but application layer DDoS attack can be a flooding attack or it can be a protocol specific vulnerability attack. There are various protocol specific vulnerability attacks which cannot be detected by traditional detection systems as they are designed to detect flooding attacks. One such type of attack is the slowloris attack which came into existence recently. It targets web servers by exploiting vulnerability in the HTTP protocol. In this report we are going to propose a detection mechanism to detect slowloris attack. We will introduce an adaptive time out based approach. There are two modules in the mechanism: Suspect Determination Module and Attacker Verification Module. Determination Module determines suspects and sends them to the Verification Module which then can verify a suspect as an attacker by using the adaptive time-out based approach. We have designed a detection algorithm which will detect an attacker before it consumes all our resources. It will detect attacker's IP address with high accuracy and low false alarm.

Keywords: *Slowloris Attack, Adaptive Time-out, DDoS Attack, HTTP Protocol.*