Project Summary: Automated DDoS Protection on the NetVM Platform

Overview

This project will lower the cost of protecting network services against Distributed Denial of Service (DDoS) attacks; it does this by eschewing specialized networking hardware in favor of the commodity Linux servers typically deployed in datacenters. In the past, commodity servers have not been fast enough to provide the performance required; as such, typical DDoS defense strategies use specialized networking hardware. However, while larger companies can afford the expense, smaller businesses are not always able or willing to pay the cost. By building a solution on top of hardware that is already commonly deployed and accessible, even smaller businesses will be able to quickly and easily deal with DDoS attacks.

The system will sit between an internal network and a larger one (e.g. a business' internal network and the Internet) with the ultimate goal of reducing the effectiveness of DDoS attacks on the internal network. The system will monitor IP traffic as it enters the internal network and rate all incoming network connections using various heuristics. Very suspicious connections that are highly reminiscent of a DDoS attack will be blocked; moderately suspicious connections will be throttled; unsuspicious connections will pass through the system untouched.

Subtopic name: IT6- Networking Technology
Keywords: IP networking, DDoS prevention, NetVM

Intellectual Merit

This Small Business Innovation Research Phase I project will develop a computer program that classifies and defends against various classes of DDoS traffic. The main technical hurdle for the program is its high performance target. In order to be competitive with the solutions it attempts to replace, the system must be able to process packets at line rate (typically 10Gbps), which will allow it to use 100% of the throughput provided by network cards commonly found in datacenters. This high performance target represents this project's main technical hurdle; it also requires that the program be highly efficient. Assuming an average size of 100 bytes per IP packet, this means that this program could be expected to process 12.5 million packets per second; in order to achieve this throughput, the program must process each packet in just 80 nanoseconds.

Broader/Commercial Impact

For a company with business-critical service such as a website, downtime directly translates to lost revenue. As such, it is very important for the business to find ways of preventing downtime, which includes protecting oneself against DDoS attacks. However, robust protection against DDoS attacks is usually not cheap. This system provides a cost-effective approach to DDoS defense through the use of NetVM, a high-performance network function virtualization platform that uses run-of-the-mill commercial-grade servers. This allows clients to take the same class of servers that run their business-critical applications and use them to protect their network from attack.