Project Summary

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, OpenNetVM

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. 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. 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 no more than 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 OpenNetVM, a high-performance networking 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.

Project Description

Elevator Pitch

This project will build Athena, a high-performance Distributed Denial of Service (DDoS) protection system on the commodity Linux servers commonly found in datacenters. The target customer for this product is a business that maintains one or more highly-available services (such as a website) and needs a method of protecting their service(s) from DDoS attacks. Other companies would invest in specialized networking hardware to deploy to their network; this customer needs a more cost-effective solution that allows them to purchase just enough capacity and scale up as necessary.

The system produced by this project fits the target customer's needs exactly. Athena runs on commodity x64 Linux servers; the customer already has many of these running their business critical applications. Because of this, the customer already has the expertise needed to provision, deploy, and maintain these servers; there's no need to train employees on a new technology. The system is also horizontally scalable; this means that the business can adjust the system's capacity by adding or removing servers.

Two key innovations of this system are its flexibility and familiarity. The system can be easily deployed and upgraded using a process similar to that of any other program running in the target customer's datacenter. This means the system administrators employed at the datacenter will already be familiar with the basics of the system. The main innovation for this system, however, is the performance; using modern CPUs and the high-performance networking platform OpenNetVM, the system will be able to process packets at line rate (typically 10Gbps) and use 100% of the network bandwidth provided by the server.

The Commercial Opportunity

The Market

For every record-breaking DDoS attack, there are many more that are smaller in scale. These smaller DDoS attacks don't make headlines, but are still very capable of taking down smaller businesses if they are unprepared. Athena specifically targets small DDoS attacks that aren't necessarily massive in scale, but still large enough to cripple a service. Businesses that would be potential targets for this scale of DDoS attack form the total addressable market for this product.

The typical business in this product's addressable market is a medium-to-large sized enterprise business that operates one or more highly-available services. This business's goal is to adequately protect themselves against smaller scale DDoS attacks while paying as little as possible for protection. To achieve this goal, this business will use one of three solutions: 1) employ no DDoS protection at all, 2) build a solution in-house, or 3) pay for the services of a commercial content-distribution network (such as CloudFlare or Akamai). Businesses that have chosen solution 1 currently undervalue the financial cost of a DDoS attack and will likely undervalue the product. Businesses that have chosen solution 2 have already invested heavily in a custom solution, and will likely be less willing to throw away the current investment in favor of another approach. Businesses that have chosen solution 3 form the initial target market for this product. The businesses in this category have invested money into DDoS protection and therefore understand its value; however, they also understand its cost and will be more easily convinced to pursue a less costly solution.

Analysis of Competition

The product's closest competitors are the services of content-distribution networks (CDNs). A CDN is a network of geographically-distributed proxies. Their main purpose is to lower the latency a user sees when interacting with a website; however, they also offer DDoS protection as a side-effect. Although there is overlap in target markets, our product hopes to compete with other CDNs entirely on the basis of price. By pricing Athena deployments much lower than that of their CDN-equivalent offerings, this product will target the lower-end of the commercial CDN market.

Business Model and Potential for Risk

The project will initially offer two products, both of which cater to the initial target market: an installer for the software and a server with the software already installed on it (a so-called "appliance"). The installer offers the most control to customers by allowing them to deploy the software to servers however they please. The appliance offers less control but eases the process of deploying the product to a datacenter. A yearly subscription that provides software updates will also be offered.

By the time the product is ready for the market, the number of large DDoS attacks will have increased. More DDoS attack-related news headlines will increase awareness of the negative effects of DDoS attacks; businesses will see other businesses gaining bad publicity and losing money. They will want to avoid the same fate for themselves, and their search for solutions will increase demand in the target market.

The product's ability to compete in the target market is heavily dependent on its price; as such, unexpected costs in developing the software pose a large potential risk to the project. The cost of development represents the key factor in determining the cost of the product; if the product is too expensive to produce, the resulting high price will drive away interest. It is critical that costs are kept down.

Broader Impact

The recent large DDoS attacks on public Internet companies have been breaking records and making news headlines. These large DDoS attacks are terrible for businesses, as they result in downtime and lost income. DDoS attacks are bad for the Internet as a whole as well; they encourage smaller businesses to hide behind DDoS mitigation services and contribute to the centralization of the Internet. This project hopes to provide a potential alternative to traditional CDNs, and help society by contributing to Internet decentralization.

Technical Discussion and R&D Plan

The key technical challenge faced by this product is the development of an algorithm for detecting DDoS attacks. Since this product is meant to be placed directly between the Internet and the customer's network, it must operate without slowing down the customer's connection to the Internet. For the purposes of our research we have assumed that the customer has a 10Gbps connection to the internet; in this case, it means that the product could be expected to process up to 30 million packets per second for patterns that indicate malicious attacks. This places a very high performance requirement on the core algorithm – it must be able to consistently analyze a single packet in less than 30 nanoseconds.

In addition to being highly performant, Athena must also meet a related requirement: it must be scalable. Performance refers to how quickly and efficiently Athena's algorithms execute on a single processor core; as such, improvements to performance increase the capacity of a single processor core. Scalability refers to the relationship between the number of processor cores running the system and the system's capacity. The more scalable a system is, the closer the ratio between cores and capacity is to 1. In a 100% scalable solution, there is a completely a linear relationship between core count and capacity; doubling the number of processor cores will result in a doubling of system capacity. In order to remain cost-effective, Athena must be as highly scalable; in other words, adding more servers ("scaling out") or improving the processors in the current server pool ("scaling up") should increase the capacity of the system as much as possible. If Athena cannot scale easily and cheaply, it won't be able to keep up with the increasing scale of DDoS attacks.

Technical Innovations

Athena's main technical innovation lies within its use of general-purpose processors. In the past, the performance requirements of certain networking tasks (such as DDoS detection and packet switching) have been handled with specialized hardware that can keep up with the rate of network traffic. Modern general-purpose processors, however, have become much faster and are now a feasible solution for this class of problems. Although it makes it harder to achieve target performance, Athena's use of commodity x64 processors represents its greatest advantage over other solutions: it allows Athena to provide the same features at a significantly lower cost.

Technical Milestones

Athena's first technical milestone is an effective defense against protocol DDoS attacks. Protocol attacks attempt to abuse network protocols to overwhelm and confuse a target server. Athena's first step toward this protocol attack defense is the implementation of TCP replay, a feature which attempts to detect and block SYN flood protocol attacks. When a TCP connection is opened on a network, a 3-way TCP handshake must be completed before the connection is considered established. To begin the handshake, the client side of the connection sends a SYN packet to the server. In response to a SYN packet, a TCP server will typically allocate some memory to begin tracking the connection state. During a SYN flood, the target server will receive a large amount of bogus SYN packets. Each incoming SYN packet causes the server to allocate some memory and wait for the rest of the TCP handshake; eventually, the target server allocates all of its memory and crashes. With TCP replay, Athena will intercept and

complete the TCP handshake on behalf of the target server. Once the connection is established and vetted, Athena will forward the connection to the server.

Volumetric DDoS attacks represent Athena's second technical milestone. As the name implies, volumetric attacks attempt to overwhelm a target server through sheer volume of network traffic. During a volumetric attack, the target server will dutifully try to process the massive flood of incoming requests. For each request that the target server processes, however, several more will come in. Over time, the target server will spend more time struggling to keep up with the attacker's requests, and less time handling requests from other users. This is a different failure scenario than that of a protocol attack; victims of protocol attacks run out of resources and crash, while victims of volumetric attacks slow to a crawl. This is because unlike protocol attacks, volumetric DDoS attacks generate valid requests. This means that defending against this class of attacks requires a more sophisticated approach than that required of protocol attacks; simple validity checking will not be enough. If Athena is able to detect these types of attacks with a moderate degree of accuracy, it can divert the overwhelming flood of requests away from the target server.

R&D Plan

The first set of R&D goals for this project center around understanding the uses (and abuses) of common network protocols. The first research goal is to study the TCP implementations used in common operating systems. Due to its popularity, the TCP protocol has been extended with various options that attempt to optimize its performance. Each TCP implementation supports a different set of TCP options; by adding support for common options, Athena may be able to take advantage of performance optimizations hidden in the TCP protocol. The second research goal is to learn the characteristics of common protocol and volumetric attacks. By conducting DDoS attacks in a controlled environment, we can analyze network metrics and develop heuristic algorithms for DDoS detection.

The second set of R&D goals for this project center around optimization. Athena's optimization plan targets three separate parts of the project. The first optimization target is the DDoS detection code used by Athena to determine when a DDoS attack is affecting the network. The second set of optimization targets involve Athena's use of the ONVM platform API. Although significant effort has been spent on optimizing OpenNetVM itself and the libraries it depends on, it is worth pursuing optimization of the interface between ONVM and Athena's DDoS code. The last major optimization target is the architecture of the application itself; Athena must be designed in a way to ensure scalability on modern multi-core systems.

Revisions made

In my draft proposal, the "Technical Discussion and R&D Plan" section is only one paragraph; in my final draft I'll make sure to expand this section. I'll also go through the whole paper and make sure that all domain-specific technical terms are explained thoroughly; I want my proposal to be understood even by those without a technical background in Computer Science. I also need to do some rearranging of a few oddly-phrased sentences here and there.