



Information System Security Operation

NetBouncer

Client-legitimacy-based High-performance DDoS Filtering

Overview

The "NetBouncer" project is an approach and set of technologies for providing practical and high-performance defenses against distributed denial-of-service (DDoS) attacks. The central innovation in the NetBouncer approach to filtering and mitigating DDoS attacks is the ability to distinguish legitimate from illegitimate traffic so as to enable the discarding of only illegitimate traffic. In particular, this allows a NetBouncer-enabled network to distinguish DDoS congestion from flash crowd congestion situations. This provides a unique advantage over other DDoS mitigation techniques such as those based on filtering and congestion control where some loss of legitimate traffic is inevitable.

The NetBouncer approach is characterized as an end-point-based solution to DDoS protection. It provides localized protection at potential choke points or bottlenecks that may exist in front of hosts and servers. NetBouncer attempts to block traffic as close to the victim as possible, while upstream of the nearest bottleneck.

The immediate manifestation of NetBouncer technology is as a high-speed packet processing in-line appliance based on network processor technology. However, the long-term evolution, adoption, and integration of NetBouncer technology may be in the back-plane/fast path of commercial high-speed routers and other packet processing devices.

Objectives and Approach

NetBouncer is being designed to provide a DDoS defense solution that can meet the scalability and performance needs of high bandwidth, real world, commercial, and military

environments. The objective is to create a solution that:

- Is easy to integrate and deploy.
- Is scaleable in terms of network topology complexity and network speeds.
- Imposes minimal administrative overhead.
- Requires minimal collaboration across organizations and network infrastructure and Internet service providers.

Central to the NetBouncer design is the ability to distinguish legitimate from illegitimate traffic, and the ability to prioritize their processing in a manner such that legitimate packets are given highest priority service. A successful NetBouncer is independent of individual DDoS attack and vulnerability specifics.

Innovative Features

NetBouncer approach and design incorporate several innovative elements including:

- DDoS mitigation based on testing for the legitimacy of network traffic using legitimacy tests and offering advantages over both anomaly and signature-based mitigation.
- Monitoring of traffic, based upon Quality-of-Service (QoS) and context-based parameters.
- Hardware-assisted high-speed packet processing techniques and architectures using network processors so as to achieve high throughputs.
- QoS related traffic management schemes to provide rate- limiting and bandwidth management for various classes of traffic based on client legitimacy and service priorities.

The legitimacy tests do not require any changes to the configurations of clients and servers. The design team has experimented with a number of

This work sponsored by DARPA through SPAWAR, Contract Number N66001-01-C-8046.

complimentary legitimacy tests to assess their efficacy in real-world high-performance settings. Each NetBouncer device may potentially maintain a very large legitimacy list, which will be continuously updated to reflect various locality conditions on the source IP addresses that are originating requests to a target set of servers.

Current Status

The NetBouncer project has made progress in three areas:

- Designed and implemented a variety of legitimacy tests to mitigate some of the most popular DDoS attacks. These include Internet Control Message Protocol (ICMP) Echo Floods, SYN Floods, Smurf and code red style attacks,
- Domain Name Service (DNS) Reflection Floods and Real Time Control Protocol (RTCP) Flood attacks on video streaming services. Built a high-speed prototype using the Intel IXP1200 network processor. Depending on the traffic mix, the prototype

can sustain throughputs in the range of 298 Mbps to 990 Mbps.

- Conducted extensive performance and analysis experiments under various attack scenarios.

Technology Transition

We are currently seeking opportunities to demonstrate NetBouncer features and conduct pilot programs with NetBouncer technology within the government as well as the private sector. In preparation for this, NetBouncer is currently undergoing red team evaluations. We focus on providing intrusion protection technology for its customers offers excellent opportunities for "productization" of NetBouncer and related techniques so as to complement existing intrusion protection products. McAfee® has applied for five patents associated with the work SPARTA's Security Research Division, then, McAfee Research, performed on NetBouncer.

We welcome opportunities to demonstrate and to conduct pilot programs using NetBouncer technology.

