Demo Description:

NetBouncer: Client-legitimacy-based High-performance DDoS Filtering

Roshan Thomas, Hong Zhu, Tim Huck, Tommy Johnson

Network Associates Laboratories
1145 Herndon Parkway, Suite 500
Herndon, VA 20170

NetBouncer is a research project currently under funding by the Fault Tolerant Networks (FTN) program within DARPA. The project is developing a set of innovative technologies to enable organizations to defend against distributed denial-of-service (DDoS) attacks. 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.

In its current form, NetBouncer technology consists of high-speed packet processing and filtering devices built on top of leading-edge network processor technology. The key innovation of the NetBouncer approach is the ability to distinguish legitimate traffic from illegitimate traffic. To enable filtering of incoming packets, a NetBouncer device maintains a large legitimacy list of clients that have been proven to be legitimate. If packets are received from a client (source) not on the legitimacy list, a NetBouncer device will proceed to administer a variety of legitimacy tests to challenge the client to prove its legitimacy. If a client can pass these tests, it will be added to the legitimacy list and subsequent packets from the client will be accepted until a certain legitimacy window expires. Once accepted, the transmission of legitimate packets is controlled by a traffic management subsystem that applies various bandwidth allocation and rate limiting schemes to ensure that legitimate clients do not abuse bandwidth consumption and that target servers cannot be overwhelmed even by what appears to be legitimate traffic.

The NetBouncer technology demonstration consists of two phases. In the first phase, we will set up a scenario where a client machine successfully sends requests to a server. We will then initiate one or more well-known DDoS attacks simulated to come from hundreds of attacking machines and directed to the server. This will result in the server being overwhelmed and not being able to service legitimate requests from clients. In the second phase, we will insert a NetBouncer device on the fly and between the client and the server. The device will proceed to issue one or more legitimacy challenges on the attack traffic and successfully mitigate the DDoS attack by distinguishing and filtering the illegitimate attack traffic. At each stage of the demo, we will use automated traffic analysis tools to present visual traffic maps that give the viewer a clear idea of the status and progress of the demonstration.