



FloodWatch: Distributed Denial-of-Service Detection and Response

Automated Defense against Zero-Day DDoS Attacks

Overview

Distributed Denial-of-Service (DDoS) attacks are a critical threat to large IP-based networks. Powerful DDoS toolkits are available to potential attackers, and essential networks are ill prepared for defense. To meet the increasing need for detection and response to zero-day DDoS attacks, McAfee® Research, now the Security Research Division of SPARTA, and Boeing Phantom Works developed a solution to statistically discriminate DDoS traffic from legitimate traffic in routers or other network devices. Once distinguished, DDoS traffic is subject to focused rate-limiting or packet filtering to mitigate the downstream effects of the attack. Our DDoS defense approach requires no predefined signatures, explicit coordination between defending network components, built-in knowledge of applications of protocols, or instrumentation at end hosts. It can complement other approaches using these techniques in a comprehensive DDoS defense solution.

Objective

The DDoS Tolerant Networks project objective was to develop technology for routers to detect and react to DDoS attacks, enabling network self-healing. This project focused on mechanisms that can be deployed in high-speed routers and mechanisms that are effective against future stealthier DDoS attacks. We addressed two primary problems:

- Identification of statistical measures that are both efficient to compute, and effective at detecting traffic that contributes to a DDoS attack multiple network “hops” back from the attack target.

- Development of attack-profiling and filtering algorithms that discard a high percentage of DDoS traffic and a low percentage of legitimate traffic. Given these two sets of algorithms, it becomes feasible to integrate DDoS defense into routers or network intrusion detection devices to create self-healing networks.

Developed Technology

FloodWatch, the DDoS defense system developed under this project, is an integrated detection and response system that has been shown effective against current DDoS attack tools and some stealthier variants. The detection module measures statistical properties of specified fields in packet headers, watching for anomalies that may indicate DDoS attacks. This module computes two statistics:

- Entropy (a measure of randomness of a set of values); and
- Divergence of frequency-sorted distributions from a baseline using the chi-square statistic.

Both of these statistics are compared to statistics from a baseline traffic sample. Analysis of live Internet traffic traces has shown that these statistics fall within predictable ranges while a network is not under DDoS attack, but move outside these ranges when DDoS attacks are introduced.

These two statistics are simultaneously computed on a set of header values from a stream of network packets. Either statistic can trigger a DDoS alert, leading to an automated response from the FloodWatch response module. While the detection module is computing its statistics, it also computes attack signatures describing the packets contributing to significant fluctuations in the statistics.

This work sponsored by DARPA through SPAWAR under Boeing Phantom Works, Contract Number N66001-01-C-8048.



FloodWatch: Distributed Denial-of-Service Detection and Response

Automated Defense against Zero-Day DDoS Attacks

These signatures enable fine-grained attack packet-filtering in the response module. FloodWatch was initially developed for Linux and was then integrated into Intel IXP and CloudShield network processors to validate that the algorithms are efficient enough to support on-line analysis at line rates in core network routers. The team developed a simulation using the ns-2 network simulator to assess the potential effectiveness of FloodWatch in large networks.

While FloodWatch is primarily targeted at the DDoS threat, it is also applicable to rapid, random-scanning worms such as Slammer. To evaluate this claim, the team developed a tool to simulate Slammer behavior on a large network of networks. Experiments with this tool showed that FloodWatch effectively detected and blocked the spread of Slammer without the use of predefined signatures or other built-in knowledge of this worm.

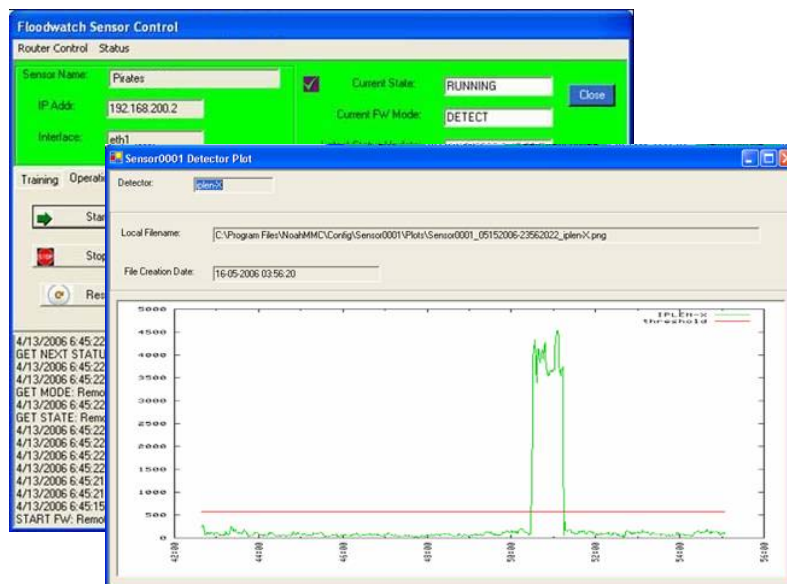
FloodWatch was selected by the Air Force Information Operations Battlelab as a Concept Demonstration. In this 2006 demonstration, a 30+ node Air Force testbed was configured to model a multi-segment base network connected injected through both live traffic replay and automated application stimulation. A

Government red team designed and carried out various attacks (external and insider) to assess the suitability of FloodWatch to operational networks. The demonstration was successful; FloodWatch was shown to accurately detect and respond to the DDoS attacks.

SPARTA developed a remote management capability for FloodWatch devices in response to Government requirements. This management console was used successfully by Air Force operators to configure, operate, and monitor FloodWatch for the Battlelab demonstration.

FloodWatch Capabilities

- FloodWatch algorithms can be employed in core routers to defend against DDoS floods.
- FloodWatch is efficient enough to run at line speeds on network processor platforms.
- FloodWatch computes statistics on the packets flowing through a router to detect DDoS attacks on the network.
- When an attack is launched, FloodWatch automatically generates an attack signature and applies focused rate-limiting rules.
- FloodWatch mitigates attack impact downstream while preserving network availability for legitimate traffic.



FloodWatch management console showing a detected DDoS attack