Phalanx: Defending Against Multimillion-node Botnets

Distributed Denial of Service (DDoS) Attacks

A large number of attackers (usually compromised end-hosts) “floods” a server like Estonia.gov. Since the server cannot serve all the requests, it serves requests at random.

As most of the requests are illegitimate, the good users get only a small amount of service. In extreme cases, all requests time out and nobody gets any service at all.

State of the Art

Cacheable content can be massively replicated using commercial systems like Akamai, CoDeeN or Coral. The approach is that with enough servers with enough bandwidth that they simply stand up to the attack.

Introducing Mailboxes

Phalanx leverages a similar set of servers to those used above, but uses them as “mailboxes” to store and forward traffic rather than serve content.

Rather than sending traffic directly to the server, it is first sent to a “mailbox” where it is held for the server to pick it up or eventually dropped. This places the recipient in control of what traffic it receives.

Many such mailboxes are used for each flow, preventing there from being a single point of failure. Either machines or links.

Mitigating Attacks

If excessive losses are detected, the data rate can be increased by adding redundancy using either FEC or retransmits. This enables the losses to be masked and normal operation to continue.

Evaluation

The cumulative fraction of mailboxes seeing at most a given loss rate. Defending with 7200 mailboxes with 100 Mb access links and filters deployed at a tier-1, we can handle a million-node botnet.

The fraction of acceptable connections (those with less than 3% loss) for both Phalanx and a TVA-like, single-path solution with the same deployment. Using a single path means some connections always see high loss.

Dynamic Content

Many current services are not replicable or cacheable, but still require protection. VoIP, AJAX web applications, e-commerce, and e-government are a few examples.