Weathering SYN Floods Using RESPIRE

András Korn, Dr. Gábor Fehér, Judit Gyimesi

A few years ago, numerous major e-commerce sites were successfully brought down using an attack called SYN flooding. This type of attack is substantially less expensive for the attacker than a bandwidth attack, because it is sufficient to fill the TCP backlog of the victim; using up all available bandwidth is not required. A number of methods for combating SYN floods have been proposed, many of which are widely deployed. In this paper, we describe a possible enhancement to some of these techniques; a way to automatically detect, isolate and filter SYN floods while conserving resources on the victim. We demonstrate its effectiveness using a call-level simulation and mathematical analysis.

Our approach requires no additional data-gathering equipment to be deployed. Rather, it makes use of the data the victim itself must collect anyway in order to be able to provide TCP service.

We assume that during a SYN flood, the ratio of the number of outgoing SYN ACK packets to the number of incoming handshake-finishing ACK packets is going to be much larger than one. Note that most SYN ACK packets that go unacknowledged are sent to the attackers; thus, we can identify the attackers by finding the subnet with the most outgoing SYN ACKs per incoming ACKs.

We address this problem by storing per-netblock SYN ACK and ACK counters in an efficient, dynamically expandable hierarchical data structure that exploits the hierarchical nature of IP space: a 256-ary tree.

We demonstrate that it is possible to detect, isolate and block high-intensity floods very quickly (less than half a second). We also prove that the reaction time of the algorithm improves as the intensity of the attack increases.