Abstract

In this paper we provide an integrated defense solution that enables filtering and admission challenges to be implemented in a distributed manner throughout the network on behalf of the target. The admission challenge is provided through the client puzzles employed at the target. This scuttles any attempt made by the attacker to flood the target because until the client solves the puzzle it isn’t granted access to the targets resources. If the attack persists or worsens, then the target could propagate a distress signal upstream to its Internet Service.
New Integrated Approach for Mitigating DDOS Attacks

Provider (ISP), who could deploy proxy defenses at the ingress points to the ISP's network on behalf of the target. In general, the target's ISP could request other upstream ISPs to also deploy the defenses for the target by using the pushback technique, so that the attack traffic is blocked as close as possible to the source of the traffic. A key advantage of this proposed approach is that it could enable the defenders to harness greater computational resources in order to counteract the growth in attack power that is becoming available to attackers.

References

- Fu-Yuan Lee, Shiu-hyung shieh. "Defending against spoofed DDOS attack with path fingerprint," www.elsevier.com/locate/cose
- I. Clarke, O. Sandberg, B. Wiley, and T. Hong, "Freenet: A Distributed
New Integrated Approach for Mitigating DDOS Attacks

- Steven Bellovin. ICMP traceback messages. IETF draft-bellovin-itrace-00. txt
- S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," in 11th USENIX Security Symposium (Security &apos;02), 2002.

Index Terms

Computer Science
Security
Keywords
Client Puzzle  Pushback  Integrated Approach