Abstract

DDoS attacks have been haunting the Internet security over a decade. The current trend shows that DDoS attack frequency is increasing with time. Over the years many researchers have proposed a wide range of different mechanisms to defend against different types of DDoS attacks. These solutions usually make different assumptions of the problem for example, some of them assumes the solution to be independent of the intermediate network while others assume cooperation from the intermediate routers. Similarly, the computational model used in these defense solutions also varies widely. In this thesis, I discuss different aspects of a DDoS defense system. First, I propose a near real time DDoS detection system. However, to mitigate a DDoS attack the defense system should be able to not only detect the attack but also discriminate the attack packets from normal packets. Keeping such a requirement in mind, I discuss a DDoS defense system based on the bidirectional nature of Internet communications. In the thesis I also address the issue of detecting spoofed attack packets from benign packets. I also discussed a log based traceback mechanism to reveal the actual source(s) of the attack packets. To carry out my experiments I developed a tool called TUCANNON to generate different types of DDoS attack traffic in test bed environment. The tool is presented as an appendix of the thesis.

Keywords — DDoS attack, DDoS attack Tool, DDoS attack detection, anti spoofing technique, traceback, DDoS mitigation, DDoS defense