ABSTRACT

From the past two decades Denial-of-Service attack continues to be the most challenging problem in the Internet. Very little efforts are required for the execution of a DoS attack, since a large number of vulnerable machines on the internet provide a fertile ground for attackers for launching such attacks. Also the availability of vast number of exploitation tools, automated scripts add to the misery as these tools and scripts can easily be used for vulnerability exploitation and the launching of DoS attacks. At the receiving end of DoS attack is the victim machine, who in case of a successful attack is deprived of its rightful state of working. The victim machine can be any machine from a standalone host to an information system catering to the needs of thousands of legitimate clients. The primary target of DoS attack is dismantling the security structure that exists in and around of an information system or any host machine. In the process a majority of security parameters get affected, one of them is AVAILABILITY. AVAILABILITY, together with CONFIDENTAILITY and INTEGRITY, has been the most critical component of information security for over three decades now and has suffered more at the hands of DoS attacks than the other security attributes, but ironically has received very low attention as compared to the other security attributes.

The primary goal of the research is to investigate the impact of DoS attacks on AVAILABILITY. A through study on AVAILABILITY is needed so that the factors that determine AVAILABILITY can be identified. The importance of AVAILABILITY as a security attribute in the information security paradigm and its critical relation with the other security attributes remains the driving point throughout the study, given the current state of AVAILABILITY in theory and practice as a security attribute. After the identification of AVAILABILITY determinants, they need to be tested against DoS attacks, for the study and analysis of the question "how DoS attacks affect AVAILABILITY?" to validate the answer, certain experiments were conducted in the thesis. Basically this study helped in understanding the theatrics of DoS attacks in a better way, which is important considering the need of an efficient DoS defense scheme.

While measuring the Availability if we go beyond the application level of an information system i.e. the component level, the dependencies that exist among the various interacting components in the software of an information system, can be used to determine the availability/workability or risk analysis of an information system. Work in the thesis presents a component level metric based on the dependencies among interacting components, the metric quantifies the availability of the information system. The metric gives an idea about the risk involved (from the security perspective) in the particular design of the component composition. The first part of the research accomplishes the above mentioned facts.

The second part of the research investigates the Denial-of-Service problem in detail, in the context of users accessing services over Internet and Networks. The attack structures used to orchestrate single source DoS attacks and Distributed source DoS attacks are discussed. In order to understand the various attack trends and accordingly create a ground for the design of a prevention strategy, a study of frequently occurring DoS attacks in recent years (2012 - 2016) was carried out and TCP-SYN DoS attack was seen as the most prolonging and frequently occurring attack in the recent time. In order to devise a prevention scheme for TCP-SYN attack, some well know prevention techniques were studied in detail. Based on the study Packet Filtering was seen as the most effective technique against the TCP-SYN attack. Next a study on the existing filtering techniques was carried and based on the study it was decided that there exists a greater scope for improvement in the Hop-Count-Filtering technique. Based on the study a *Victim Based Statistical Filtering (VBSF)* technique for the prevention of TCP-SYN type of DoS attacks is proposed in the thesis. An Algorithm is also given for the proposed technique in the thesis, followed by the validation using a small scale experiment under controlled conditions. The filtering technique after evaluation showed promising results.