Chapter 7

Conclusion and Future Scope

7.1 Conclusion Drawn

The impact of Denial of Service attack on *Availability*, can result in affecting all other security attributes of information security and if the problem of DoS attacks is not addressed with a quick response, the consequences for an organization can be enormous. The problem of DoS attacks is un-avoidable in the present architecture of *Internet*, the only thing that can be done is mitigating the effect and make the techniques more efficient with the changing times and technologies.

In order to minimize the gap that exists between Availability and other security attributes, in understanding their theory and application perspectives, we present a thorough understanding and analysis in chapter 2. Given the importance of availability in the information security paradigm, the security stakeholders should treat the three attributes of security i.e. *confidentiality*, *integrity* and *availability,* equally in their respective domains wherever they are applicable. In-fact while dealing with *information security* more attention is needed for *availability* as a security attribute given its importance and the dependence of other security attributes on *availability* and moreover without availability of the information/information-system one cannot apply the methods of security like *Authentication, Encryption, Hashing, Access-Methods* etc. Since availability is applicable in software, hardware and the network, the measurements regarding systems availability in all the three cases can be done both at the system level (as a whole) and the individual component levels. Critical information processing systems are always trying to achieve continuous availability, which is very hard to maintain. While as most of the information processing systems settle down for high availability. Basic availability is the lowest achievable form of availability.

For analyzing the impact of DoS attacks on *Availability*, the factors identified at the Service/System level of an information system are; *Reliability, Timeliness* and *Accessibility*. To measure and analyze these three factors, there exists a good number of metrics in the literature. A single parameter was picked from these metrics for the analysis of DoS attacks on availability via these system level factors. After conducting experiment-

1 using Sockstress stress testing framework, it was observed that *Reliability* was affected when the system was brought down by the DoS attack (downtime). *Timeliness* was affected by the linear increase in ICMP response time on the legitimate machine. The other way of looking at the effect on *timeliness* is downtime also. For testing *Accessibility* we used the *Siege* framework and focused on three parameters of siege i.e. *concurrency, response-time* and *availability.* With respect to the question, “how many concurrent connection does the server support?” we conclude with the fact that there exists a relation between *concurrency, response-time* and *availability,* the parameters of requests to the server. Higher number of concurrent connections are possible only when the response time of every user request is low, preferably below the universally accepted mark (refer to table 1 for the universal standard operation requirement). The vice versa is true as well, when the response time is high, the concurrency is low. Now under normal conditions in the system the response time will mostly be under permissible limits, which therefore won’t affect the number of concurrent connections that a server can support. But going by the results of table 23 on the experiment 1, a DoS attack can severely impact the response time (ICMP response time or RTT) and in the table we have seen how the response time jumped beyond the permissible limits once the attack was launched. It even reached to infinite (server unreachable). Now once the response time starts increasing, the availability and concurrency start decreasing. In other words the increase in response time leads to decrease in the number of concurrent connections that a server can support. In worst cases very high response time will lead to no concurrent connections or no connections at all, leading to what we call as a Denial of Service Attack and thus affecting *Accessibility.*

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 chapter 4 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. Besides quantifying the availability of individual components, a classification of every component based on the availability score is also done. It will help in keeping a close eye on the performance of the critical components as critical components would easily be identified by their availability scores. Metric incorporates the component interactions of the system, processing time of every component and in case of remote-component composition, the delay associated with every component. Heavy interactions among components can affect availability, if the components with critical availability scores are called upon again and again, it may result in low performance and may ultimately impact the workability/availability of the information system. Using certain performance metrics of software/information systems, we can use the results of performance with the results from the availability metrics as a reference and if need be the design may be altered for better performance of the information system.

In order to provide a solution to the problem of DoS attack in the internet, a deeper understanding and analysis of the problem is needed. Chapter 5 presents a deeper look into the problem and summarizes the different attack structures used by both single source DoS attacks and Distributed source DoS attacks. The chapter also analyses the state of DoS attacks in the recent years (2012-2016), we found TCP-SYN as the most frequently occurring DoS attack, followed by UDP flood, DNS amplification, ICMP flood and the newly rising NTP amplification. By this analysis we can very efficiently plan the defense expenditure as we can analyze the attack trends and always keep eye on the weaker points in the internet. The amplification attacks continue to be the most devastating form of DoS attacks (distributed in nature) on the internet present today. The ICMP, UDP and TCP-SYN flooding attacks showed a constant downfall of around 20% between the periods 2012-2016.

The *Victim Based Statistical Filtering* mechanism can produce greater results provided, an efficient port monitoring scheme is developed that can closely monitor the activity levels of the port numbers on the destination machine. The strength of the VBS Filtering mechanism lies in this information, therefore more efficient and optimal information gathering we have much efficient will be the filtering process. Also one thing should be taken into the consideration, the port monitoring processing should not overwhelm the server itself, otherwise the defense may also fall prey to the attackers and they might use this feature also for the attack.

7.2 Recommendations for Future Work

The work in the thesis leaves a sizable scope for further research. This section marks some suggestions for further research and some of the limitations that exist in the work done in the thesis.

1. Data analysis in experiment 1 can be improved further by replicating the experiment and recording the state of TCP buffer space on the server. The state of the server can also be analyzed by launching the attack from distributed sources.
2. The evaluation results of Algorithm 2 in chapter 4 can be improved by minimizing the assumptions made in *InDeg(Ci)* and *outDeg(Ci)*. Since the metric is more inclined towards the software part of the information system, the future scope lies in incorporating more of the other components (hardware, user and network) in the metric as well. Also in the future the work can be extended to distributed computing environment, which involves a complex component based architecture of hardware, software and the network.
3. For the detailed and complete analysis of DoS attack problem in the internet, more attack statistics needs to be analyzed. Chapter 5 contains statistics of DoS attacks from the past 5 years, more statistics can help in better understanding of attack trends and accordingly new ideas for the mitigation can be put forward.
4. The *VBSF* technique needs to be implemented, tested and analyzed in a live scenario to measure the actual performance over the existing HCF and other techniques. Port monitoring on the destination machine is not used seriously as an additional tool in the existing filtering techniques to thwart DoS attacks as it can overwhelm the server by its processing, however adding a separate dedicated hardware processing support for port monitoring can make the port monitoring information more usable in the future, as its efficient use can greatly improve all

the victim based filtering techniques. The time quantum that should be allocated for the analysis of a port number for activity levels is still an unanswered question, an optimal time scale needs to be developed so that the filtering mechanism accurately capture the falsified IP packets.