

- [3] J. Lemon, "Resisting SYN Flood DoS Attacks with a SYN Cache," *Proceeding of the 10th ACM SIGOPS European Workshop*, pp. 89-97, 2002.
- [4] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007.
- [5] Z. Qian and Z. Mao, "Off-Path TCP Sequence Number Inference Attack," in *IEEE Symposium on Security and Privacy*, 2012, pp. 347-361.
- [6] W. Eddy, "Defenses Against TCP SYN Flooding Attacks," *Cisco Internet Protocol Journal*, vol. 9, no. 4, december 2006.
- [7] V. Jacobson, "Pathchar: A tool to infer characteristics of internet paths," Network Research Group, Berkeley, CA, May 1997.
- [8] V. Paxson and M. Allman, J. Chu, and M. Sargent, "Computing TCP's Retransmission Timer," RFC 6298 (Proposed Standard), June 2011.
- [9] V. Anil Kumar, G. Patra, and R. Thangavelu, "On Remote Exploitation of TCP Sender for low-rate flooding denial-of-service attack," *IEEE Communications Letters*, vol. 13, no. 1, January 2009, pp. 46-48.
- [10] N. Hubballi, S. Biswas, S. Nandi, "Towards Reducing False Alarms in Network Intrusion Detection Systems with Data Summarization Techniques," *International Journal on Security and Communication Networks*, vol.6, no.3, 2013, pp. 275-285.
- [11] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the Shrew vs. the Mice and Elephants," *ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, vol.1, 2003, pp. 75-86.
- [12] A. Kuzmanovic and E. W. Knightly, "Low-rate tcp-targeted denial of service attacks and counter strategies," *IEEE/ACM Trans. Netw.*, vol. 14, no. 4, pp. 683-696, 2006.
- [13] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," *IEEE Communications Letters*, vol. 9, no. 4, pp. 363-365, april 2005.
- [14] H. Sun, J. C. S. Lui, and D. K. Y. Yau, "Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection," in *Proceedings of IEEE Conference on Network Protocols (ICNP 2004)*, pp. 196-205, 2004.
- [15] J. Liu and M. Crovella, "Using Loss Pairs to Discover Network Properties," in *Proceedings ACM Internet Measurement Workshop*, 2001, pp. 127-138.
- [16] C. L. Schuba and E. H. Spaord, "A Reference Model for Firewall Technology," in *Proceedings of the 13th Annual Computer Security Applications Conferene (ACSAC)*, 1997, p. 133.
- [17] R. Sekar, M. Bendre, D. Dhurjati, and P. Bollineni, "A Fast Automaton-Based Method for Detecting Anomalous Program Behaviors," in *IEEE Symposium on Security and Privacy*, Oakland, California, 2001, pp. 144-155.
- [18] Y. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "Hawk: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions From Shrew DDOS Attacks," in *Proceedings of the 3rd International Conference on Networking and Mobile Computing (ICNMC 2005)*, Springer – Verlag, New York, 2005, pp. 423-432.
- [19] C. Chang, S. Lee, B. Lin, and J. Wang, "The Taming of The Shrew: Mitigating Lowrate TCP-Targeted attack," *IEEE Transactions on Network and Service Management (TNSM)*, vol. 7, no. 1, pp. 1-13, 2010.
- [20] S. Savage, N. Cardwell, D. Wetherall, and T. Anderson, "TCP Congestion Control with a Misbehaving Receiver," *ACM Computer Communicaitns Review*, vol. 29, October 1999, pp. 71-78.
- [21] R. Sherwood, B. Bhattacharjee, and R. Braud, "Misbehaving TCP Receivers can Cause Internet Wide Congestion Collapse," in *ACM Conference on Computer and Communications Security*, 2005, pp. 383-392.
- [22] A. Ramaiah, R. Stewart, and M. Dalal, "Improving TCP's Robustness to Bline in-Window Attacks," RFC 5961 (Proposed Standard), August 2010.
- [23] C. G. Cassandras and S. Lafortune, "Introduction to Discrete Event Systems, Springer, 2nd edition, 2008.
- [24] S. Whitaker, M. Zulkernine, and K. Rudie, "Towards Incorporating Discrete-Event Systems in Secure Software Development," *The 3rd International Conference on Availability, Reliability and Security*, IEEE, 2008, pp. 1188-1195.
- [25] K. Cheng and A. Krishnakumar, "Automatic functional test generation using the extended finite state machine model," in *Proceedings of 30th Design Automation Conference*, Dallas, Texas, USA, ACM Press, 1993, pp. 86-91.
- [26] NS2, The Network Simulator. <http://www.nsnam.isi.edu/nsnam/> [Retrieved on January, 2014].