{tag} {/tag}

IJCA Proceedings on International Conference on Information and Communication Technologies

ICICT - Number 4

Year of Publication: 2014

Authors:
Karthik Pai B. H

Nagesh H

Abhijit Bhat

{bibtex}icict1434.bib{/bibtex}

Abstract

One of the biggest concerns for security professionals today are Distributed Denial of Service (DDoS) flooding attacks. They are nothing but explicit attempts to disrupt the legitimate users' access to services. One of the more popular DDoS attack is the SYN Flood attack. The SYN flooding attacks are launched by exploiting the TCP's three-way handshake mechanism and its limitation in maintaining its half-opened connections. The

proposal is to present a simple and robust mechanism that detects the SYN flooding attacks with less computational overhead. The two algorithms which would be used are an adaptive threshold algorithm and the cumulative sum (CUSUM) algorithm for change point detection. The proposal is to measure the performance in terms of the packet delivery fraction. The evaluation results are presented in NS2 simulation environment.

References

- H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks", in Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM), volume 3, pp. 1530-1539, June 23-27, 2002.
- MitkoBogdanoski, Tomislav Shuminoski and Aleksandar Risteski " Analysis of the SYN Flood DoS Attack" I. J. Computer Network and Information Security, 2013, 8, 1-11 Published Online June 2013 in MECS (http://www. mecs-press. org/)DOI: 10. 5815/ ijcnis. 2013. 08. 01.
- D. M. Divakaran, H. A. Murthy and T. A. Gonsalves, "Detection of SYN Flooding Attacks Using Linear Prediction Analysis", 14th IEEE International Conference on Networks, ICON 2006, pp. 218-223, Sep. 2006.
- V. A. Siris and P. Fotini, "Application of Anomaly Detect Algorithms for Detecting SYN Flooding Attack" Elsevier Computer Communications, pp. 1433-1442, 2006.
- S. Gavaskar, R. Surendiran and Dr. E. Ramaraj, "Three Counter Defense Mechanism for SYN Flooding Attacks", International Journal of Computer Applications, Volume 6–No. 6, pp. 12-15, Sep. 2010.
- SamanTaghaviZargar, James Joshi and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks.
- C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram and D. Zamboni, "Analysis of a Denial of Service Attack on TCP", Proceedingsof IEEE Symposium on Security and Privacy, May 1997.
- T. Nakashima and S. Oshima, "A detective method for SYN flood attacks", First International Conference on Innovative Computing, Information and Control, 2006.
- D. Nashat,X. Jiang and S. Horiguchi, "Detecting SYN Flooding Agents under Any Type of IP Spoofing", IEEE International Conference on e-Business Engineering table of contents, 2008.
- W. Chen and D. -Y. Yeung, "Defending Against SYN Flooding Attacks Under Different Types of IP Spoofing", ICN/ICONS/MCL '06, IEEE Computer Society, pp. 38-44, April 2006.
- A. Yaar, A. Perrig and D. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense", IEEE Journal on Selected Areas in Communications, Volume 24, no. 10, pp. 1853-1863, October 2006.
- S. -W. Shin, K-Y. Kim and J. -S. Jang, "D-SAT: detecting SYN flooding attack by two-stage statistical approach", Applications and the Internet, pp. :430 – 436, 2005.
- J. Haggerty, T. Berry, Q. Shi and M. Merabti, "DiDDeM: a system for early detection of SYN flood attacks", GLOBECOM, 2004.
- J. Haggerty, Q. Shi and M. Merabti, "Early Detection and Prevention of

Denial-of-Service Attacks: A Novel Mechanism With Propagated Traced-Back Attack Blocking", IEEE Journal On Selected Areas In Communications, Vol. 23, No. 10, pp. 1994-2002, October 2005.

- S. Qibo, W. Shangguang, Y. Danfeng and Y. Fangchun, "An Early Stage Detecting Method against SYN Flooding Attacks", China Communication, Vol. 4, pp. 108-116, November 2009.
- G. Wei, Y. Gu and Y. Ling, "An Early Stage Detecting Method against SYN Flooding Attack", International Symposium on Computer Science and its Applications, pp. 263-268, 2008.
- P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1. , Lawrence Livermore National Laboratory, February 14, 2000.
- Yahoo on Trail of Site Hackers, Wired. com, Feb. 8, 2000,[online]http://www. wired. com/news/business/0, 1367, 34221,0. html.
- Powerful Attack Cripples Internet, Oct. 23, 2002, [online] http://www. greenspun. com/bboard/q–and–a–fetch–msg. tcl?msgid=00A7G7
- Mydoom lesson: Take proactive steps to prevent DDoS attacks,Feb. 6,2004,[online]http://www. computerworld. com/s/article/89932/Mydoom lesson Take proactive steps to prevent DoSattacks? taxonomyId =017.
- Lazy Hacker and Little Worm Set Off Cyberwar Frenzy, July 8, 2009,[online] http://www. wired. com / threatlevel /2009 /07/ mydoom/
- New "cyber attacks" hit S Korea, July 9, 2009, [online] http://news. bbc. co. uk/2/hi/asia-pacific/8142282. stm
- Operation Payback cripples MasterCard site in revenge for WikiLeaks ban, Dec. 8, 2010, [online] http://www. guardian. co. uk / media/2010/dec/08/operation–payback–mastercard–website–wikileaks
- T. Kitten, DDoS: Lessons from Phase 2 Attacks, Jan. 14, 2013, [online] http://www. bankinfosecurity. com/ddos-attacks-lessons-from-phase-2-a-54 20/op-1.
- L. Garber, "Denial-of-Service Attack Rip the Internet", Computer, April 2000.
- Check Point Software Technologies Ltd. SynDefender: http://www. checkpoint. com/products/firewall-1.
- Netscreen 100 Firewall Appliance, http:// www. netscreen . com/
- D. Moore, G. Voelker and S. Savage, "Inferring Internet Denial of Service Activity", Proceedings of USENIX Security Symposium'2001, August 2001

Index Terms

Computer Science Security

Keywords
Cusum Algorithm Ns2