Network Flow-Based Anomaly Detection of DDoS Attacks

Georgios Androulidakis, gandr@netmode.ntua.gr
Vasilis Chatzigiannakis, vhatzi@netmode.ntua.gr
Mary Grammatikou, mary@netmode.ntua.gr
Fotis Stamatelopoulos, fotis@netmode.ntua.gr

Network Management and Optimal Design (NETMODE) Lab, National Technical University of Athens, Iroon Polytexneiou 9, 15780 Zografou, Greece

Keywords: Intrusion Detection, Distributed Denial of Service Attacks, Anomaly Detection

Abstract

Denial of Service (DoS) attacks do not attempt to break into computer systems but aim to the disruption of the normal system operation through overloading network and / or system resources [1]. Their complexity and magnitude is rapidly increasing and their distributed version (DDoS attacks) is becoming a nuisance to modern IT infrastructure and a very challenging detection problem [2]. Various detection solutions are proposed and many intrusion detection tools attempt to identify DDoS attacks mostly through anomaly detection, i.e. identification of deviations from normal operation patterns. We present an anomaly detection solution that relies on network flow data exported from CISCO Netflow-enabled [3] devices; this work is inspired by and augments the algorithm and set of metrics initially proposed in [4].

The proposed detection algorithm monitors flow data from all interfaces of border routing equipment and calculates specific metrics that are compared against adaptive thresholds that characterize the “normal” network utilization. Metrics are calculated for each pair of input-output interfaces using “number of packets” and “number of flows” counters and their mean values. The detection algorithm generates alarms for specific interface pairs based on a boolean expression combining the metrics and the respective threshold values that adapt to changing traffic patterns. The algorithm reports interface pairs and suspected destination IP addresses affected by the detected DoS/DDoS attack; both IPv4 and IPv6 addresses are identified. We developed a prototype detection tool that implements the proposed algorithm, and ran IPv4 experiments within the Greek Research and Technology Network (GRNet – http://www.grnet.gr) as well as experimented with IPv6 traffic traces (6NET Project [5]) from the Swiss Education and Research Network (SWITCH – http://www.switch.ch).

The prototype tool consists of two main modules: the collector and the detector. The collector module is responsible for asynchronously receiving flow data from the Netflow-enabled devices; information is analyzed, mean values and adaptive thresholds are calculated and stored in a local data structure. The tool extracts and stores packet and flow counters per destination IP address, as well as total counters and mean values for each pair of input-output interfaces. The collector may be configured to “listen” to multiple sources of network flow statistics concerning both IPv4 and IPv6 traffic. The detector process is responsible for calculating the metrics for the interface pairs stored by the collector, and comparing the results to detection thresholds. It is periodically activated, implements extensive logging of detection

events and generates e-mail notifications with security alerts to the administrator. The prototype tool is implemented as a Java application and it is platform independent.

The initial experiments with the proposed algorithm and the prototype tool are very promising and we are currently experimenting further with various metrics and threshold adapting algorithms. The goal of our experiments is to identify metric sensitivity and finalize a set of metrics, adaptive thresholds and boolean expressions for providing reliable detection.

Acknowledgements

We would like to thank people from both GRNET and SWITCH for providing access to their infrastructure and network flow traces respectively.

References

1. G. Koutepas, B. Maglaris, "Detection and Reaction to Denial of Service Attacks", Cyprus Security Society "2nd Conference on Information Security: From Theory to Practice", Nikosia, Cyprus, October 2002.
2. J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defence Mechanisms," University of California, Technical Report #020018 (also available at http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf), 2002
3. Cisco IOS NetFlow, http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml
4. C. Kotsokalis, D.Kalogeras, and B. Maglaris, "Router-Based Detection of DoS and DDoS Attacks", HP OpenView University association (HPOVUA) Conference '01, Berlin, Germany, June 2001.
5. 6Net: Large-Scale International IPv6 Pilot Network, http://www.6net.org

Vitae

Georgios Androulidakis is a PhD Student at the National Technical University of Athens (NTUA). He is a Research partner in the NETwork Management and Optimal DEsign laboratory (NETMODE) of the National Technical University of Athens. His research interests include network security, intrusion detection and network management. He has a Diploma degree in Electrical and Computer Engineering from National Technical University of Athens. He is a member of IEEE and USENIX Association.

Vasilis Chatzigiannakis is a PhD Student at the National Technical University of Athens (NTUA). He works in the Network Operations Center in NTUA, is a researcher in the NETwork Management and Optimal DEsign laboratory (NETMODE) of the National Technical University of Athens and an IEEE member. His research interests include network management, network security and distributed systems. He has a Diploma degree in Electrical and Computer Engineering from National Technical University of Athens.

Maria Grammatikou is a Research Associate and Coordinator of the Network Management and Optimal Design Laboratory (NETMODE) of NTUA of Greece. She works as a teaching assistant in NTUA. Her research interests include topics on management and optimal design of computer communication networks, Security and Intrusion Detection Systems, Electronic commerce and web-based technologies,

parallel/distributed systems and communication systems evaluation. She has a PhD in Computer Science from the NTUA of Greece. She has an extensive experience in software systems design & development and she has participated in many European projects. She is a member of the WG7/TC48 Working Group.

Fotis Stamatelopoulos is a Senior Researcher at the Institute of Communication and Computer Systems, NTUA and a member of the Network Management and Optimal Design Laboratory. He has a PhD in Electrical and Computer Engineering from NTUA and an MSc in Computer Science from the University of Maryland, USA. His research interests include network and systems management, network security, middleware architectures and e-business systems.