IMPROVED PERFORMANCE HIGH SPEED NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

A high speed NIDS architectures to address limitations of Packet Loss and Low Detection Rate by adoption of Dynamic Cluster Architecture and Traffic Anomaly Filtration (IADF)

Monis Akhlaq

Submitted for the Degree
of Doctor of Philosophy

School of Computing, Informatics and Media
University of Bradford

2011

Dedicated to my beloved father, **Mr Akhlaq Ahmed**
who was the major source of inspiration to me, I miss him a lot…..

Acknowledgments

I pray and thank Almighty Allah for giving me the strength and the wisdom to complete this research, I have a firm belief that without His help this work would have not been completed.

First and foremost, I am indebted to my advisors, Mr John Mellor and Professor Irfan Ullah Awan, for the outstanding motivation, guidance, support, and knowledge that they have provided throughout the course of this work. They kindly took me into the Network Security Research Group and provided me with a great amount of freedom to work. Their confidence and trust on my abilities were the major motivating factors for this achievement.

I am also grateful to my research colleague Faeiz Alserhani for helping me throughout this long journey. His punctuality and capacity to attend the lab for long hours were the source of encouragement. His support to review my research papers and attend the presentation rehearsals cannot be forgotten. Collectively, we have made quite a few reputable publications and have also arranged conferences/ workshops.

My sincere thanks to my sponsors, National University of Sciences & Technology (NUST), Pakistan for giving me this opportunity to study abroad for this coveted qualification. My employers Pakistan Army also deserve recognition for allowing me to study abroad.

The major contributor in this achievement is my family - my lovely wife Erum, I thank you for your support and encouragement. I really appreciate your patience for accepting my absence for long hours, this must have spoiled some precious moments of our life. My naughty kids, Duaa, Manahil and Chiya also deserves pats on their back, they really supported me in this journey. I am sure my son Umar bin Monis must be celebrating these moments in his true home.

Last, but not the least I thank my parents, my mother in law, my family and friends back home in Pakistan. It has been their prayers, encouragement and support that enabled me to reach at this point.

Abstract

Intrusion Detection Systems (IDS) are considered as a vital component in network security architecture. The system allows the administrator to detect unauthorized use of, or attack upon a computer, network or telecommunication infrastructure. There is no second thought on the necessity of these systems however; their performance remains a critical question.

This research has focussed on designing a high performance Network Intrusion Detection Systems (NIDS) model. The work begins with the evaluation of Snort, an open source NIDS considered as a de-facto IDS standard. The motive behind the evaluation strategy is to analyze the performance of Snort and ascertain the causes of limited performance. Design and implementation of high performance techniques are considered as the final objective of this research.

Snort has been evaluated on highly sophisticated test bench by employing evasive and avoidance strategies to simulate real-life normal and attack-like traffic. The test-methodology is based on the concept of stressing the system and degrading its performance in terms of its packet handling capacity. This has been achieved by normal traffic generation; fussing; traffic saturation; parallel dissimilar attacks; manipulation of background traffic, e.g. fragmentation, packet sequence disturbance and illegal packet insertion. The evaluation phase has lead us to two high performance designs, first distributed hardware architecture using cluster-based adoption and second cascaded phenomena of anomaly-based filtration and signature-based detection.

The first high performance mechanism is based on Dynamic Cluster adoption using refined policy routing and Comparator Logic. The design is a two tier mechanism where front end of the cluster is the load-balancer which distributes traffic on pre-defined policy routing ensuring maximum utilization of cluster resources. The traffic load sharing mechanism reduces the packet drop by exchanging state information between load-balancer and cluster nodes and implementing switchovers between nodes in case the traffic exceeds pre-defined threshold limit. Finally, the recovery evaluation concept using Comparator Logic also enhance the overall efficiency by recovering lost data in switchovers, the retrieved data is than analyzed by the recovery NIDS to identify any leftover threats.

Intelligent Anomaly Detection Filtration (IADF) using cascaded architecture of anomaly-based filtration and signature-based detection process is the second high performance design. The IADF design is used to preserve resources of NIDS by eliminating large portion of the traffic on well defined logics. In addition, the filtration concept augment the detection process by eliminating the part of malicious traffic which otherwise can go undetected by most of signature-based mechanisms. We have evaluated the mechanism to detect Denial of Service (DoS) and Probe attempts based by analyzing its performance on Defence Advanced Research Projects Agency (DARPA) dataset. The concept has also been supported by time-based normalized sampling mechanisms to incorporate normal traffic variations to reduce false alarms. Finally, we have observed that the IADF has augmented the overall detection process by reducing false alarms, increasing detection rate and incurring lesser data loss.

Contents

Figures

Tables