Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 5, May -2016

Intrusion Detection System To Improve Security

Vishwadeep Wasekar, Chetan Baste, Prof.Dipali Patil

Department Of Computer Engineering, Sinhgad Institute of Technology, Lonavla.

Abstract *— In the last decade, design and execution of low-power systems provides brought significant attention. Started out with data centers and battery-operated mobile devices, this has recently branched to core network devices many of these as routers. However, this kind of emerging need for low-power system design has not really been studied for protection systems, which are turning into increasingly important today. Toward this direction, we purpose to reduce the electric power consumption of Network-level Protection Evaluation Systems, which usually are being used to increase the protected procedure of modern computer system networks. Unfortunately, traditional techniques to low-power system design and style, such as frequency climbing bring about a disproportionate take hold of packet processing and queuing times. In this function, we show that this kind of increase includes a negative effect on the detection dormancy and impedes a well-timed reaction. To address this problem, we present NLSES: a great architecture that resolves the energy-latency trade-off by offering both low power usage and low detection dormancy simultaneously. The key thought is to identify the packets that are extremely likely to carry a great attack and provide them larger priority to be able to achieve low attack detection latency. Each of our results indicate that NLSES consumes comparable power to a state-of-the-art low-power design and style, while, at the same time, reaching up to an order of value faster attack detection.*

Keywords*:-IDS (Intrusion Detection system)*

I. INTRODUCTION

Low power consumption has appeared as one of the key design goals in present computer systems. Recently, very much effort has been place into increasing the strength efficiency in a selection of areas like info centers, powerful computing, portable devices, and networks. Toward this direction, we make an effort to build an energy-efficient Network level Security Evaluation Program. Security Evaluation System are generally deployed to discover protection violations, boosting the protected procedure of modern computer system networks. They perform computationally heavy functions like design matching, regular expression corresponding, and other types of complex analysis to discover at real time destructive activities in the supervised network. Thus, Security Analysis System usually makes use of multi-core systems or cluster of servers to cope with increased link speeds and complicated analysis. Nevertheless, the energy efficiency of security alarm systems like NLSES has certainly not received significant attention and will not be studied before.

Typically, Security Evaluation systems intended for fixed networks were divided into two categories -- network-based and host structured Security Evaluation System. Network-based systems (NLSES) passively or perhaps actively listen on the network, and capture and examine individual packets moving through a network. Contrary to firewalls, Security Evaluation Program can analyzed the complete supply, not simply IP addresses and ports. They are in a position to look at the payload within a supply, to see which special host application has been utilized, and with what choices, also to raise alerts intended for the attacker tries to exploit a bug on such code, by discovering known attack signatures. Network Security Evaluation System will be host-independent, and may run because "black box" monitors to cover the complete networks of systems. In practice, |working scanning slows down the network considerably, and can easily effectively analyze an in short supply bandwidth network. NLSES frequently required dedicated hosts or perhaps special equipment, and so can easily be prone to the network attack. They will be able to discover activities such as repeated failed access attempts or adjustments to critical system documents or data, and normally operate simply by accessing logs or monitoring real-time system usage. To ensure effective operation, web host Security Evaluation System consumers have to be mounted on every host upon the network, focused on the subject of specific host configuration.

II. LITERATURE REVIEW

1. A Framework for DNS based detection and mitigation of malware infections on a network
Author: Etienne Stalmans.
Description:

Modern botnet trends have lead to the use of IP and domain fast-fluxing to avoid detection and increase resilience. These techniques bypass traditional detection systems such as blacklists and intrusion detection systems. DNS is one of the most prevalent protocols on modern networks and is essential for the correct operation of many network activities, including botnet activity. For this reason DNS forms the ideal candidate for monitoring, detecting and mitigating botnet activity. In this paper a system placed at the network edge is developed with the capability to detect

fast-flux domains using DNS queries. Multiple domain features were examined to determine which would be most effective in the classification of domains. This is achieved using a C5.0 decision tree classifier and Bayesian statistics, with positive samples being labeled as potentially malicious and negative samples as legitimate domains. The system detects malicious domain names with a high degree of accuracy, minimizing the need for blacklists. Statistical methods, namely Naive Bayesian, Bayesian, Total Variation distance and Probability distribution are applied to detect malicious domain names. The detection techniques are tested against sample traffic and it is shown that malicious traffic can be detected with low false positive rates.

2. An Empirical Reexamination of Global DNS Behavior
Author: Hongyu Gao, Vinod Yegneswaran, Yan Chen, Phillip Porras, Shalini Ghosh, Jian Jiang, Haixin Duan.
Description:

The performance and operational characteristics of the DNS protocol are of deep interest to the research and network operations community. In this paper, we present measurement results from a unique dataset containing more than 26 billion DNS query-response pairs collected from more than 600 globally distributed recursive DNS resolvers. We use this dataset to reaffirm findings in published work and notice some significant differences that could be attributed both to the evolving nature of DNS traffic and to our differing perspective. For example, we find that although characteristics of DNS traffic vary greatly across networks, the resolvers within an organization tend to exhibit similar behavior. We further find that more than 50% of DNS queries issued to root servers do not return successful answers, and that the primary cause of lookup failures at root servers is malformed queries with invalid TLDs. Furthermore, we propose a novel approach that detects malicious domain groups using temporal correlation in DNS queries. Our approach requires no comprehensive labeled training set, which can be difficult to build in practice. Instead, it uses a known malicious domain as anchor, and identifies the set of previously unknown malicious domains that are related to the anchor domain. Experimental results illustrate the viability of this approach, i.e. , we attain a true positive rate of more than 96%, and each malicious anchor domain results in a malware domain group with more than 53 previously unknown malicious domains on average.

3. Power Containers: An OS Facility for Fine-Grained Power and Energy Management on Multicore Services
Authors: Kai Shen, Arrvindh Shriraman, Sandhya Dwarkadas, Xiao Zhang ,Zhuan Chen.
Description:

Energy efficiency and power capping are critical concerns in server and cloud computing systems. They face growing challenges due to dynamic power variations from new client-directed web applications, as well as complex behaviors due to multicore resource sharing and hardware heterogeneity. This paper presents a new operating system facility called "power containers" that accounts for and controls the power and energy usage of individual fine-grained requests in multicore servers. This facility relies on three key techniques---1) online model that attributes multicore power (including shared maintenance power) to concurrently running tasks, 2) alignment of actual power measurements and model estimates to enable online model recalibration, and 3) on-the-fly application-transparent request tracking in multi-stage servers to isolate the power and energy contributions and customize per-request control. Our mechanisms enable new multicore server management capabilities including fair power capping that only penalizes power-hungry requests, and energy-aware request distribution between heterogeneous servers. Our evaluation uses three multicore processors (Intel Woodcrest, Westmere, and Sandy Bridge) and a variety of server and cloud computing (Google App Engine) workloads. Our results demonstrate the high accuracy of our request power accounting (no more than 11% errors) and the effectiveness of container-enabled power virus isolation and throttling. Our request distribution case study shows up to 25% energy saving compared to an alternative approach that recognizes machine heterogeneity but not fine-grained workload affinity.

4. MemScale: Active Low-Power Modes For Main Memory

Authors: Qingyuan Deng , David Meisner, Luiz Ramos, Thomas F. Wenisch, Ricardo Bianchini
Description:

Main memory is responsible for a large and increasing fraction of the energy consumed by servers. Prior work has focused on exploiting DRAM low-power states to conserve energy. However, these states require entire DRAM ranks to be idled, which is difficult to achieve even in lightly loaded servers. In this paper, we propose to conserve memory energy while improving its energy-proportionality by creating active low-power modes for it. Specifically, we propose MemScale, a scheme wherein we apply dynamic voltage and frequency scaling (DVFS) to the memory controller and dynamic frequency scaling (DFS) to the memory channels and DRAM devices. MemScale is guided by an operating system policy that determines the DVFS/DFS mode of the memory subsystem based on the current need for memory bandwidth, the potential energy savings, and the performance degradation that applications are willing to withstand. Our results demonstrate that MemScale reduces energy consumption significantly compared to modern memory energy management approaches. We conclude that the potential benefits of the MemScale mechanisms and policy more than compensate for their small hardware cost.

5. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks (2003).
Author: Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon , Kendall Nygard.
Description:

Mobile ad hoc networks (MANETs) are generally extensively consumed within military and civilian applications. your own dynamic topology of MANETs will allow nodes to help join and leave your network in any kind of point connected with time. The generic characteristic associated with MANET possesses rendered That vulnerable to be able to safety attacks. Within the particular paper, when I address your current problem connected with coordinated attack from multiple black holes acting inside group, my partner and I supply a good system to distinguish multiple black holes cooperating within each other a good method to distinguish a risk-free route avoiding cooperative black hole attack.

III. SURVEY OF PROPOSED SYSTEM

This paper proposes Security Evaluation System: this architecture that resolves the energy-latency trade off. The implementation of Security Evaluation uses NIC features, a specialized kernel module, a modified user-level library, and it is based on the popular Snort. Security Evaluation System consumes less power, proportionally to the traffic load, while its detection latency remains low and almost constant at any traffic load. The main contributions of this work are:

• We identify a new trade off for Security Evaluation System: the energy-latency trade off. As we reduce power consumption, the detection latency is significantly increased, which impedes a timely reaction to incoming attacks. We found that the main cause of this increase is the queuing delays imposed by the high core utilization.

• We resolve the energy-latency trade off by identifying the packets that have a higher probability to contain an attack and processing them with higher priority.

• We introduce space sharing: a new technique based on flow migration that processes high-priority packets in dedicated cores with low utilization, and moves the low priority packets to cores with higher utilization.

• We experimentally compare two alternative approaches for low latency in a power-proportional Security Evaluation System We show that space sharing results in lower detection latency when power consumption is reduced.

• We present the design, implementation, and evaluation of Security, a Security Evaluation System architecture that achieves both low latency and reduced power consumption.

IV. Mathematical Model

Let W is the set of whole of system which consists:

W= {input, process, output}.

Input={D, MDNS, RE, NTA}

Where,

1. D is the set of data collector.
2. MDNS is the set o malicious DNS detector which detects the malicious IP at DNS server traffic.
3. NTA is the network traffic analyzer which detects the network traffic.
4. RE is the reputation engine which calculates the reputation score of an IP address.

V. SYSTEM ARCHITECTURE

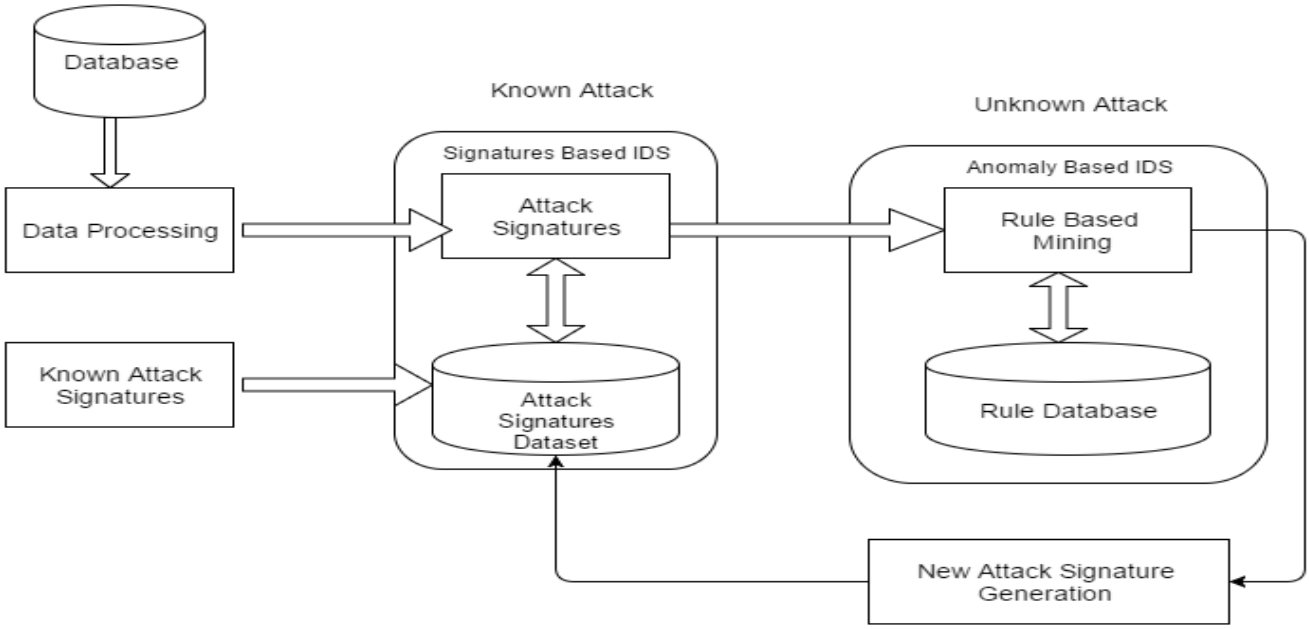

Fig. System Architecture

VI. CONCLUSION AND FUTURE WORK

From this work we studied the challenge of increasing the energy efficiency of Security Analysis System using common electric power management functions like DVFS and C-states. First, we determined an energy dormancy trade-off: the reduced electric power consumption leads to a significant increase of the recognition latency, which impedes a timely reaction of Protection Evaluation System to inbound attacks. We showed that the key reason of this increase is the high queuing delays imposed by high core utilization. After that, we presented the design, implementation, and analysis of Security Evaluation System: in that resolves the energy-latency trade-off. They key idea of Security Evaluation Strategy is to process with higher priority the first few bytes of each and every flow, which have a higher possibility to carry an harm, to accomplish lower latency for them and faster harm detection. We proposed two alternative techniques: time showing, which utilizes a typical concern queue scheduling, and space sharing, which uses dedicated cores with low usage to process high-priority bouts. Our experimental analysis shows that Security Evaluation Program performs better with space sharing, resulting in low power consumption, proportionally to the load, and constantly low attack detection dormancy simultaneously.

VII. REFERENCES

1. A. Pathak, Y. C. Hu, and M. Zhang, ‘‘Where is the energy spent inside my app?: Fine grained energy accounting on smartphones with Eprof,’’ in Proc. ACM Eur. Conf. Comput. Syst. (EuroSys), 2012, pp. 29–42.
2. Q. Deng, D. Meisner, L. Ramos, T. F. Wenisch, and R. Bianchini, ‘‘MemScale: Active low-power modes for main memory,’’ in Proc. ACM Int. Conf. Archit. Support Program. Lang. Oper. Syst. (ASPLOS), 2011, pp. 225–238.
3. F. Fusco and L. Deri, ‘‘High speed network traffic analysis with commodity multi-core systems,’’ in Proc. ACM SIGCOMM Conf. Internet Meas. (IMC), 2010, pp. 218–224.
4. V. Paxson, R. Sommer, and N. Weaver, ‘‘An architecture for exploiting multi-core processors to parallelize network intrusion prevention,’’ in Proc. IEEE Sarnoff Symp., Apr./May 2007, pp. 1–7.
5. M. Vallentin, R. Sommer, J. Lee, C. Leres, V. Paxson, and B. Tierney, ‘‘The NIDS cluster: Scalable, stateful network intrusion detection on commodity hardware,’’ in Proc. Int. Symp. Recent Adv. Intrusion Detection (RAID), 2007, pp. 107–126.
6. H. Dreger, A. Feldmann, V. Paxson, and R. Sommer, ‘‘Operational experiences with high-volume network intrusion detection,’’ in Proc. ACM Conf. Comput. Commun. Secur. (CCS), 2004, pp. 2–11.

AUTHORS

Vishwadeep Wasekar, persuing BE in *Department Of Computer Engineering at Sinhgad Institute of Technology, Lonavla.*

Chetan Baste, persuing BE in *Department Of Computer Engineering at Sinhgad Institute of Technology, Lonavla.*

