AN ALTERNATIVE APPROACH TO
COMPUTER SYSTEM SECURITY MONITORING AND ENHANCEMENT
THROUGH SYSTEM CALL SEQUENCE ANALYSIS

ABSTRACT

Modern computer systems are plagued with stability and security problems: applications lose data, web servers are hacked, and systems crash under heavy load. Many of these problems or anomalies arise from rare program behaviors caused by attacks or errors. A substantial percentage of the web-based attacks are due to buffer overflows. Many methods have been devised to detect and prevent anomalous situations that arise from buffer overflows. The current state-of-art of anomaly detection systems is relatively primitive and mainly depends on static code checking, to take care of buffer overflow attacks. For protection, Stack Guards and Heap Guards are also used in wide varieties.

This dissertation proposes an anomaly detection system, based on frequencies of system calls in the system call trace. System call traces represented as frequency sequences are profiled using sequence sets. A sequence set is identified by the starting sequence and frequencies of specific system calls. The deviations of the current input sequence from the corresponding normal profile in the frequency pattern of system calls is computed and expressed as an anomaly score. A simple Bayesian model is used for an accurate detection.

Experimental results are reported which show that frequency of system calls represented using sequence sets, captures the normal behavior of programs under normal conditions of usage. This captured behavior allows the system to detect anomalies with a low rate of false positives. Data are presented that show Bayesian network on frequency variations responding effectively to induced buffer overflows. It can also help administrators to detect deviations in program flow introduced due to errors.

The results of the investigations carried out, as well as the concepts developed were communicated and published in one Journal and presented at 5 international conferences which appear in their Proceedings.

PhD Thesis No: 8
Surekha Mariam Varghese