ABSTRACT

THESIS: ARL-VIDS Visualization Techniques: 3D Information Visualization of Network Security Events

STUDENT: Tyler Gaw

DEGREE: Master of Science

COLLEGE: Sciences and Humanities

DATE: May, 2014

PAGES: 71

Government agencies and corporations are growing increasingly reliant on networks for day-to-day operations including communication, data processing, and data storage. As a result, these networks are in a constant state of growth. These burgeoning networks cause the number of network security events requiring investigation to grow exceptionally, creating new problems for network security analysts. The increasing number of attacks propagated against high-value networks only increases the gravity. Therefore, security analysts need assistance to be able to continue to monitor network events at an acceptable rate.

Network analysts rely on many different systems and tools to properly secure a network. One line of defense is an intrusion detection system or IDS. Intrusion detection systems monitor networks for suspicious activity and then print alerts to a log file. An important part of effective intrusion detection is finding relationships between network events, which allows for detection of network anomalies. However, network analysts typically monitor these logs in a sparsely formatted view, which simply isn't effective for large networks.

Therefore, a Visual Intrusion Detection System or VIDS is an interesting solution to aid network security analysts in properly securing the networks. The visualization tool takes a log file and represents the alerts on a three-dimensional graph. Previous research shows that humans have an innate ability to match patterns based on visual cues, which we hope will allow network analysts to match patterns between alerts and identify anomalies. In addition, the tool will leverage the user's intuition and experience to aid intrusion detection by allowing them to manipulate the view of the data.

The objective of this thesis is to quantify and measure the effectiveness of this Visual Intrusion Detection System built as an extension to the SNORT open source IDS. The purpose of the visualization is to give network security analysts an alternative view from what traditional network security software provides. This thesis will also explore other features that can be built into a Visual Intrusion Detection System to improve its functionality.