

Visualization of Security Logs Project

Due Date:

Objective:

To implement a portable security log visualization tool using Java as an implementation language.

Description:

Computer forensic is the information that is produced, stored, or transmitted by a computer system or network. It is primarily the evidentiary material that is collected and used in establishing and analyzing digital transactions and activities. Once this data is collected and secured, the analysis and reporting of the data is usually required. The data analysis can be enhanced through visualization, which can be used in recognizing anomalous trends or patterns.

In this project, your group (**maximum--2 members per group**) is required to design and implement a portable visualization system for security log files. The portability requirement of the system entails the utilization of Java as the implementation language and JFreeChart, an open-source charting library, for visualization development. To accomplish this project, you need to familiarize yourself with the Netbeans IDE, Java-Swing Graphical User Interface (GUI) programming, security log file retrieval & data gathering, and JFreeChart development. The references below are provided to get you started. Also, the VizDemo application source code and a tutorial on JFreeChart can be downloaded from the course website.

References:

- [1] Erbacher, R. and Teerlink, S. "Improving the Computer Forensic Analysis Process through Visualization." Communications of the ACM. February 2006. Vol. 49.,No.2.
- [2] Axelsson, S. and Sands, D. Understanding Intrusion Detection Through Visualization. Springer-Verlag. 2005.
- [3] JFreeChart Website: <http://www.jfree.org/jfreechart/index.html>. Access date: 12/03/2006.
- [4] Deitel, et. al. Java How to Program, 6th Edition. Prentice-Hall. 2005.
- [5] Tulloch, Mitch. "Using Log Parser 2.2." Website: <http://www.windowsdevcenter.com/pub/a/windows/2005/07/12/logparser.html>. Access date: March 04, 2008.