Visualization and Management Tool for Internet Security Incident

Project Code: TD2 - 05

Project Supervisor: Prof. Danny Tsang
Group Members: Wu Hoi Man
Tsang Sai Cheong
Yim Shun
**Project Overview**

**Introduction**

As the number of enterprises which provide e-business via internet is increasing, the internet security management becomes more important.

- Security management can protect the information asset of a company.
- Companies face the threat of being attacked by hackers or virus.
- Protecting internal information is essential.
- A Visualization and Management tool for internet security incident is an urgent need for a company.

Our FYP has been sponsored by DataCog Corporation Limited ([www.dataCog.com](http://www.dataCog.com)) to develop a visualization tool for security incidents.

**Aim and Objective**

DataCog Corporation Limited has developed an auto-correlation system in log analysis across different security vendors, so the aim of our FYP includes:

- Write a program for displaying correlation of security events.
- This program must have a user-friendly and visualization interface.
- Use graphs, tree nodes, maps, paths and windows to represent complex Log message from the security incidents.
- Focus on how to help the users to understand the huge amount of correlation results.
Methodology

We have divided the project into four main tasks:

➢ **Task 1: Analyzing the SQL data:**

The data coming from the SQL are rude; We used MySQL to create a database for our project. Fig.1 shows the configuration window of MySQL.

➢ **Task 2: Designing a user-friendly interface**

Display the correlation results from a user-friendly and visualization point of view.

Fig. 1 Start to configure MySQL server.

➢ **Task 3: Visual Display:**

We aim to design an algorithm to display the information in a graphic approach. Fig. 2 is one example of using graph to display information.

➢ **Task 4: Adopted Programming Languages:**

We import several APIs into Eclipse, eg. Jgraph (Fig 3), RCP (Rich Client Platform), SWT (Standard Widget Tool), JAVA and Eclipse

Fig. 2 Example of using graphical approach to display information.

Fig. 3 Jgraph is one of the APIs we used in this project.
Implementation

The programming language of our FYP is JAVA. We implement our FYP by the software development kit (SDK) called Eclipse. Eclipse is available from an open source community.

The website of Eclipse is http://www.eclipse.org/

SWT and RCP

We used the Java library Standard Widget Toolkit (SWT) and Eclipse Rich Client Platform (RCP) to implement an attractive interface.

Result

1. Data Extraction:

We are given a set of dummy data which are arranged in the form of SQL. We have extracted the useful data and applied the data to the interface.

2. Graphical Approach:

The graphical approach is successful. We have created a graph on the GUI. Fig.4 shows the graph which generates on the GUI.

Fig.4 Circular graphic approach

3. Detail information display:

When user clicks on the node we successfully display the information of the node on the GUI. Fig.5 shows an example of detail node information.

Fig.5 Example of showing node information