Programa Institucional de Bolsas de Iniciação Científica PIBIC
23 a 25 outubro
Pró-Reitoria de Pesquisa - Pibic/CNPq
Pró-Reitoria de Graduação - SAE/Unicamp
Ginásio Multidisciplinar da UNICAMP
XXI congresso de iniciação científica da unicamp
congresso 2013

T1310

USO DA TÉCNICA TREEMAP COMO SUPORTE À ANÁLISE DE BASES DE DADOS DE MALWARE

Tatiane Zinsly, Celmar Guimarães da Silva e Profa. Dra. Regina Lúcia de Oliveira Moraes (Orientadora), Faculdade de Tecnologia - FT, UNICAMP

A manutenção de uma base de dados de *malware* não é uma tarefa trivial, se considerarmos o volume de informações que esse tipo de base armazena para garantir um alto grau de confiabilidade e ajudar no desenvolvimento, análise de cobertura e na melhoria de um antivírus. Uma base de dados de *malware* guarda informações sobre os eventos de infecções capturados pelo antivírus. Entretanto, a visualização simultânea desse tipo de informação é dificultada pela quantidade de dados existentes. A técnica *Treemap* foi escolhida para auxiliar nesta situação. Ela pode ser apropriada, considerando o fato de que ela é baseada em representação hierárquica de dados, estruturados em árvores. A técnica permite uma ampla visualização dos dados coletados e permite também uma navegação interativa por entre a hierarquia. Cada nó é representado por um retângulo e cada nó filho é representado internamente no nó pai. Características gráficas de cada nó podem ser usadas para representar dados adicionais. Área e cor dos nós são exemplos dessas características. O objetivo do uso desse tipo de gráfico é identificar padrões e tendências no comportamento dos programas maliciosos existentes atualmente e, consequentemente, auxiliar na melhoria dos produtos de segurança que combatem essas ameaças.

Malware - Database - Information visualization