Enhancing Software Reverse Engineering with Graph Neural Networks

Tech ID: 34154 / UC Case 2023-717-0

CONTACT

Edward Hsieh
hsiehe5@uci.edu
tel: 949-824-8428.

OTHER INFORMATION

KEYWORDS

software reverse engineering, binary analysis, cross-architecture, machine learning, graph neural network

CATEGORIZED AS

- **Computer**
  - Security
  - Software

RELATED CASES

2023-717-0

BRIEF DESCRIPTION

CFG2VEC is a novel Hierarchical Graph Neural Network approach designed to significantly improve the analysis of vulnerable binaries in software reverse engineering.

FULL DESCRIPTION

CFG2VEC introduces a cutting-edge technique for software reverse engineering by employing a Hierarchical Graph Neural Network (GNN) based method. This technology utilizes a unique Graph-of-Graph (GoG) representation to analyze binary functions across various CPU architectures, significantly enhancing the process of identifying and predicting function names in stripped binaries. Built as a plugin for the Ghidra reverse engineering tool, cfg2vec leverages hierarchical graph embedding and siamese network-based supervised learning to outperform existing tools in function name prediction and generalization across unseen CPU architectures.

SUGGESTED USES

· Enhanced tools for cybersecurity professionals and reverse engineers analyzing vulnerable software.

· Automated identification and patching of security vulnerabilities in mission-critical embedded software.

· Advanced academic research in the fields of machine learning, cybersecurity, and software development.

· Integration into existing software analysis and development tools to improve efficiency and accuracy.

ADVANTAGES

· Superior accuracy in function name prediction, outperforming the state-of-the-art

· Ability to generalize across various CPU architectures with a single training model.

· Significant improvement in performance with increased training data, achieving better results.

· Facilitates the analysis of binaries built from unseen CPU architectures.

· Integrates seamlessly with Ghidra, enhancing its functionality for reverse engineers.

PATENT STATUS

Patent Pending

RELATED MATERIALS

» S. -Y. Yu, Y. G. Achamyeleh, C. Wang, A. Kocheturov, P. Eisen and M. A. Al Faruque, "CFG2VEC: Hierarchical Graph Neural Network for Cross-Architectural Software Reverse Engineering," 2023 IEEE/ACM 45th International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP), Melbourne, Australia, 2023, pp. 281-291, doi: 10.1109/ICSE-SEIP58684.2023.00031.