THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

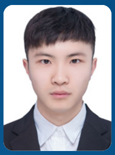
COMP RESEARCH STUDENT SEMINAR

Date : 28 November 2024 (Thu)
Time : 3:00 pm - 4:00 pm
Venue : PQ703 (Face-to-face)

DeepInfer: Deep Type Inference from Smart Contract Bytecode

Abstract

Smart contracts play an increasingly important role in Ethereum platform. It provides various functions implementing numerous services, whose bytecode runs on Ethereum Virtual Machine. To use services by invoking corresponding functions, the callers need to know the function signatures. Moreover, such signatures provide crucial information for many downstream applications, e.g., identifying smart contracts, fuzzing, detecting vulnerabilities, etc. However, it is challenging to infer function signatures from the bytecode due to a lack of type information. Existing work solving this problem depended heavily on limited databases or hardcoded heuristic patterns. However, these approaches are hard to be adapted to semantic differences in distinct languages and various compiler versions when developing smart contracts. In this paper, we propose a novel framework DeepInfer that first leverages deep learning techniques to automatically infer function signatures and returns. The novelties of DeepInfer are: 1) DeepInfer lifts the bytecode into the Intermediate Representation (IR) to preserve code semantics; 2) DeepInfer extracts the type-related knowledge (e.g., critical data flows, constant values, and control flow graphs) from the IR to recover function signatures and returns. We conduct experiments on Solidity and Vyper smart contracts and the results show that DeepInfer performs faster and more accurate than existing tools, while being immune to changes in different languages and various compiler versions.



Mr Kunsong ZHAO
PhD candidate
Department of Computing

About the Speaker

Mr Kunsong ZHAO received his B.Eng. degree from Hubei University in 2019 and his M.Eng. degree from Wuhan University in 2022. He is currently a PhD student in the Department of Computing at The Hong Kong Polytechnic University, under the supervision of Prof. Daniel Xiapu Luo. His research interests include blockchain and smart contract security, binary analysis, and software engineering.

Graph Anomaly Detection at Group Level: A Topology Pattern Enhanced Unsupervised Approach

Mr Xing AI
PhD candidate
Department of Computing

About the Speaker

Mr Xing AI received his bachelor's and master's degree in Software Engineering from Xiamen University in 2019 and 2022, respectively. He is currently pursuing a PhD in the Department of Computing at The Hong Kong Polytechnic University, under the guidance of Dr Kai ZHOU. His research centres around AI Security, Graph Learning and Graph Neural Networks.

Abstract

Graph anomaly detection (GAD) has achieved success and has been widely applied in various domains, such as fraud detection, cybersecurity, finance security, and biochemistry. However, existing graph anomaly detection algorithms focus on distinguishing individual entities (nodes or graphs) and overlook the possibility of anomalous groups within the graph. To address this limitation, this paper introduces a novel unsupervised framework for a new task called Group-level Graph Anomaly Detection (Gr-GAD). The proposed framework first employs a variant of Graph AutoEncoder (GAE) to locate anchor nodes that belong to potential anomaly groups by capturing long-range inconsistencies. Subsequently, group sampling is employed to sample candidate groups, which are then fed into the proposed Topology Pattern-based Graph Contrastive Learning (TPGCL) method. TPGCL utilizes the topology patterns of groups as clues to generate embeddings for each candidate group and thus distinct anomaly groups. The experimental results on both real-world and synthetic datasets demonstrate that the proposed framework shows superior performance in identifying and localizing anomaly groups, highlighting it as a promising solution for Gr-GAD.

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

COMP RESEARCH STUDENT SEMINAR

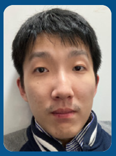
Date : 28 November 2024 (Thu)
Time : 3:00 pm - 4:00 pm
Venue : PQ703 (Face-to-face)

Finding Manipulatable Bottlenecks in Blockchain Clients

Abstract

Blockchain clients are the fundamental element of the blockchain network, each keeping a copy of the blockchain's ledger. They play a crucial role in ensuring the network's decentralization, integrity, and stability. As complex software systems, blockchain clients are not exempt from bottlenecks. Some bottlenecks create new attack surfaces, where attackers deliberately overload these weak points to congest client's execution, thereby causing denial of service (DoS). We call them manipulatable bottlenecks. Existing research primarily focuses on a few such bottlenecks, and heavily relies on manual analysis. To the best of our knowledge, there has not been any study proposing a systematic approach to identify manipulatable bottlenecks in blockchain clients.

To bridge the gap, this paper delves into the primary causes of bottlenecks in software, and develops a novel tool named ThreadNeck to monitor the symptoms that signal these issues during client runtime. ThreadNeck models the clients as a number of threads, delineating their inter-relationship to accurately characterize the client's behavior. Building on this, we can identify the suspicious bottlenecks and determine if they could be exploited by external attackers. After applying ThreadNeck to four mainstream clients developed in different programming languages, we totally discover 13 manipulatable bottlenecks.



Mr Shuohan WU
PhD candidate
Department of Computing

About the Speaker

Mr Shuohan WU received his Bachelor's degree in Computer science from Zhejiang University of Technology in 2019, followed by a Master's degree from The Hong Kong Polytechnic University in 2021. He is currently pursuing his PhD in the Department of Computing at The Hong Kong Polytechnic University, under the supervision of Prof. Daniel Xiapu Luo. His research interest focuses on program analysis, software testing, and Web3 security.