Evaluating Disassembly Ground Truth Through Dynamic Tracing (abstract)

Lambang Akbar Wijayadi, Yuancheng Jiang, Roland H.C. Yap, Zhenkai Liang, Zhuohao Liu
National University of Singapore
Email: {lambang, yuancheng, ryap, liangzk}@comp.nus.edu.sg, liu_zhuohao@u.nus.edu

***Abstract*—Disassemblers play a crucial role in reverse engineering, malware analysis, binary analysis, malware detection, binary-level security mechanisms, etc. It is well known that in general, disassembly is an undecidable problem, so errors in a disassembler should be expected. In applications where disassembly of a binary is only the first step, any disassembly errors will impact the correctness or effectiveness of tasks such as static binary instrumentation, binary hardening, binary CFI, automated code repair, etc. As such, determining what errors may lie in the disassembly of a given binary would help in determining to what extent such applications are affected by disassembly errors. Existing works have highlighted limitations and errors in existing disassemblers but they largely rely on practical implementation without specific guarantees. In this initial work, we investigate an alternative and complementary approach, where the error evaluation has a soundness guarantees. There are intrinsic tradeoffs when trying to determine the ground truth of disassembly given its theoretical undecidability. Essentially one can choose between soundness or completeness. In this work, we focus on exploring the soundness direction. We propose TraceDis which uses dynamic execution to find disassembly errors and evaluate whether TraceDis is successful to answer the following questions: (i) can TraceDis find errors consistent with existing studies evaluating disassemblers using approaches which do not have guarantees; (ii) can (new) interesting errors be found; (iii) can errors in non-C/C++ binaries be found; and (iv) can errors in closed source binaries be found. The experiments show that TraceDis finds errors in all these cases. We believe that this preliminary evaluation taking a soundness based approach shows promise. It can also complement and be an alternative to existing evaluation techniques.**

Workshop on Binary Analysis Research (BAR) 2024
1 March 2024, San Diego, CA, USA
ISBN 979-8-9894372-0-7
https://dx.doi.org/10.14722/bar.2024.23013
www.ndss-symposium.org