Assessing Software Weakness Detection Capabilities: An Empirical Study of IKOS

Hripsime Hovhannisyan, Gayane Mirakyan, Edgar Khachatryan, Hayk Aslanyan

Center of Advanced Software Technologies, Russian-Armenian University, Yerevan, Armenia

hripsime.hovhannisyan@rau.am, mirakyan.gayane@rau.am, khachatryan.edgar@rau.am, hayk.aslanyan@rau.am

***Abstract*—Memory-related vulnerabilities, such as use-after-free and double-free errors, remain a critical security issue in C and C++ programs, potentially leading to arbitrary code execution and data corruption. While dynamic analysis offers high precision, it often incurs significant overhead; conversely, static analysis provides broader coverage but faces challenges with false positives and complex memory modeling. This paper evaluates the capabilities of IKOS, a static analysis tool developed by NASA, in detecting these memory errors. We assess IKOS using the standardized Juliet Test Suite, focusing on its handling of flow, context, and path sensitivity. Our results indicate that IKOS achieves high detection rates, with an average F1 score of 95.46% for double-free and 89.67% for use-after-free scenarios. However, the analysis reveals limitations in IKOS's ability to handle complex C++ containers and global variables. This study details the specific coding patterns that cause false negatives—such as wide character usage and widening techniques in loops—providing insights for practitioners selecting the IKOS analysis tool and researchers improving static analysis precision.**

Keyword—Double-Free, IKOS, Juliet Test Suite, Memory Vulnerabilities, Static Analysis, Use-After-Free

Hripsime Hovhannisyan received her B.Sc. and M.Sc. degrees in informatics and applied mathematics from Yerevan State University, Armenia, in 2019 and 2021, respectively. With nearly six years of experience in software development, she specializes in security, demonstrating proficiency in both code static and dynamic analysis. Her research interests include graph theory, software security, and software testing. She has been pursuing a Ph.D. degree at the Russian-Armenian University since 2024.

Gayane Mirakyan received the B.Sc. degree in informatics and applied mathematics from Russian–Armenian University, Armenia, in 2024, where she iscurrently pursuing the M.Sc. degree in system programming. In 2021, she joined the Center of Advanced Software Technologies, as a Laboratory Assistant. Her main responsibilities in this role involve the development and testing of static analysis tools. Her research interests include software engineering, software static analysis, and software testing.

Edgar Khacatryan is currently pursuing the bachelor’s degree in informatics and applied mathematics with Russian–Armenian University. In 2024, he joined the Center of Advanced Software Technologies, as a Laboratory Assistant. His main responsibilities in this role involve the development and testing of static analysis tools. His research interests include software engineering, software static analysis, and software testing.

Hayk Aslanyan received the B.Sc. and M.Sc. degrees in informatics and applied mathematics from Yerevan State University, Armenia, graduating in 2014 and 2016, respectively. He obtained a Ph.D. degree in 2019 in mathematical and software support for computing machines, complexes, and computer networks from Ivannikov Institute for System Programming, Russia. Currently, he is a lecturer and researcher at the Russian-Armenian University, Armenia. His research interests include program static and dynamic analysis, software security, and compiler optimization.