Symbolic Execution For Control Flow Path Feasibility

Hovhannes Movsisyan*, Hripsime Hovhannisyan*, Hayk Aslanyan*

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

hovhannes.movsisyan@rau.am, hripsime.hovhannisyan@rau.am, hayk.aslanyan@rau.am

***Abstract*—This article presents an approach for verifying the feasibility of program control flow paths using symbolic execution. To improve the practicality of symbolic execution for our goal, we introduce techniques for automatic symbolization targeting four key areas: variables with unknown values, function arguments, return values, and pointer-referenced memories. We also propose an algorithm for verifying program paths that utilizes these enhancements and improves scalability by eliminating redundant program branches. This feature is designed for integration into static analysis tools to boost accuracy.**

***Keyword*— automatic symbolization, path feasibility, path verification, static analysis, symbolic execution**

Hovhannes Movsisyan received his B.Sc. and M.Sc. degrees in informatics and applied mathematics from Yerevan State University, Armenia, in 2019 and 2021, respectively. He joined the System Programming Laboratory at Yerevan State University in 2017 as a student. From 2022, he has been a researcher and teaching assistant in the system programming department at the Russian-Armenian University, Armenia. His research interests include symbolic execution, program static and dynamic analysis. He has been pursuing a Ph.D. degree at the Russian-Armenian University since 2024.

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.

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.