Artificial Software Diversification for WebAssembly

JAVIER CABRERA-ARTEAGA

Licentiate Thesis in [Research Subject - as it is in your ISP]
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden [2022]

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framläges till offentlig granskning för avläggande av licentiatexamen i [ämne/subject] [veckodag/weekday] den [dag/day] [månad/month] [år/2022] klockan [tid/time] i [sal/hall], Electrum, Kungl Tekniska högskolan, Kistagången 16, Kista.

TRITA-ICT XXXX:XX • ISBN XXX-XX-XXXX-XXX-X

Abstract

has become the fourth official web language. This new language allows web browsers to execute existing programs or libraries written in other languages, such as C/C++ and Rust. Apart from web browsers, evolves to be part of Edge-Cloud computing platforms. Despite being designed with security as a premise, it is not exempt from vulnerabilities. Our approaches deal with this fact by providing a preemptive solution with software diversification.

In this thesis, we propose an automatic approach to generate software diversification for programs. In addition, we provide complementary implementation for our approaches, including a generic LLVM superdiversifier that potentially extends our ideas to other programming languages. We empirically demonstrate the impact of our approach by providing Randomization and Multivariant Execution (MVE) for . Our results show that our approaches can provide an automated end-to-end solution for the diversification of programs. The main contributions of this work are:

- We highlight the lack of diversification techniques for WebAssembly through an exhaustive literature review.
- We provide the implementation of two tools, CROW and MEWE. These tools provide randomization and multivariant execution for respectively.
- We include *constant inferring* as a new code transformation to generate software diversification for .
- We empirically demonstrate the impact of our technique by evaluating the static and dynamic behavior of the generated diversification.

Our approaches harden observable properties commonly used to conduct attacks, such as static code analysis, execution traces, and execution time. Therefore, our approaches harden unknown and yet-unknown vulnerabilities.

Keywords: WebAssembly, Software Diversification, Automatic Software Engineering, Security

TRITA-ICT XXXX:XX • ISBN XXX-XX-XXXX-XXX-X