Exploring WebAssembly Security Model (DD2525)

Atheer Salim & Milad Farahani

April 2024

Background

WebAssembly (WASM) is a relatively new technology that makes it possible to run code in various languages like C and Rust directly in web browsers without any (large) notable drop in performance. How WASM does this is that it defines a binary instruction format for a stack-based VM, where the source language is code compiled to a WASM module, which is then loaded into the WASM VM that runs the code.

The Goal of the Project

The project aims to investigate the security model of WebAssembly by exploring how WASM runs code in an isolated environment within the browser. We will look at how security works and behaves in WASM, this is mostly theoretical but also practically examines attacks that are performed in/using WASM and how they can be mitigated. Overall, the goal is to gain insight into how attackers might exploit WASM, and how attacks and defenses in WASM

Relevance to language-based security

In essence, this project combines language-based security and web development. Analyzing the security model of WASM and the potential threats and defenses underlines the importance of language design to achieve secure execution in web applications.

Overview of the planned work

The overview can be summarized as follows

- Research/Study on how security works in WASM
- Research various attacks with corresponding defenses in WASM
- Implement multiple attacks as a proof of concept
- Summarize our findings

Schedule

Our schedule has the following outline, here we are having 1 week as margin if some task takes longer than expected to perform.

- **Learn WebAssembly (in general)** time frame: 1 week
- **Learn The Security Model of WebAssembly** time frame: 1 week
- **Explore Attacks in WebAssembly** time frame: 1 week
- **Implement Proof of Concept Attacks** time frame: 1 week
- **Analyze Investigation & Write Report** time frame: 1 week

Target grade

The target grade we are aiming for is **C**. This project will demonstrate a grasp of the concepts of WebAssembly security. The project will explore attacks and defences in WASM with an attack implemented as a proof of concept. The attack will be analyzed with the defences that can be used to mitigate the attack.