A framework to automatically detect vulnerabilities in WASM binaries based on known vulnerabilities by combining deep learning-based static binary analysis with dynamic binary analysis.

Known Vulnerability Detection for WebAssembly Binaries

Pengfei Sun, Luis Garcia, Yi Han, Saman Zonouz, Yao Zhao
F5 Networks, USC ISI and Rutgers University

WASP Overview

Main Idea
- Deep learning is used to train the vulnerability detector;
- The vulnerability detector is used to statically analyze the target WASM binary;
  - WASP leverages a trained multilayer perceptron (MLP) followed by the cross-entropy between the softmax outputs to determine if the two are similar.
- The identified vulnerable subroutines are run for in-depth dynamic analysis and verification of the existence of a vulnerability.
  - WASP leverages IDA Pro and Wasabi to run the CVE vulnerable function binary as well as the target Wasm function binary on identical input values.

Problem Setting and Challenges
- CVE-2018-14550
  - get_token() in libpng
- The belong figure highlights the syntactic differences between the x86 binary assembly code representation and WASM assembly code representation.

Preliminary Result and Future Work
- Six different CVEs have been evaluated. WASP can identify the correct matches among the top 3 ranked outcomes 100% of the time.
- Evaluating WASP on the aforementioned large dataset of real-world WASM binaries to characterize vulnerabilities in the wild.