Overview

This repository contains the source code behind the NDSS '22 paper "Cross-Language Attacks", available here.

The paper shows that adding code in "safe" langauges such as Rust to applications in unsafe lanaguage such as C/C++ may undermine hardening techniques that have been applied to the C/C++ code. This paradoxical result shows the importance of having well thought out and consistent threat models. Here we provide the proofs of concept referenced in the paper, for both Rust and Go. We also provide the analysis scripts we used to gauge how prevalent these vulnerabilities might be in Firefox.

Objective

The objective of this project is to aid authors of multi-language software applications in hardening their code. Securing such applications effectively requires understanding the threat model that they face, and how different defenses compose. We hope that our exploration of this subject results in more secure software.

Directory Layout

rust-cla-examples

In this directory, one can find a mixed language application (MLA) with both Rust and C code that is vulnerable to a number of Cross Language Attacks (CLAs). The C side of the program can either be compiled as a static library (libinit.a) or a dynamic shared library (libinit.so). Furthermore, the C library is compiled with Control Flow Integrity (CFI) to prevent code-reuse attacks. However, the C code contains a series of spatial memory corruption out-of-bound errors (OOB) and temporal corruption use-after-free (UAF) or double free errors that an attacker can leverage to degrade the spatial and temporal safety of Rust or by-pass the CFI protection on the C library.

go-cla-examples

In this directory, one can find another mixed language application (MLA) with both Go and C code that is vulnerable to a number of Cross Language Attacks (CLAs). Similar to the Rust MLA example, the C side of the program can be compiled separately as a static library (libinit.a) or a dynamic shared library (libinit.so). In fact, these CLA examples contain a similar set of attacks as the Rust MLA.

cla-metrics

A series of scripts to analyze mixed-language binaries for metrics that indicate the opportunity for a Cross-Language Attack (CLA).

Disclaimer

Cross-Language Attacks is distributed under the terms of the MIT License DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Under Secretary of Defense (USD) for Research & Engineering (R&E) under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of USD (R&E).

The software/firmware is provided to you on an As-Is basis