HAKC-NDSS2022

Overview

This repo contains our implementation of the compartmentalization scheme described in our NDSS '22 paper here. In the paper, we showed that compartmentalization vulnerabilities are the most common class of CVEs, and developed a novel enforcement mechanism for compartmentalization policies. Our mechanism leverages ARM MTE and PAC, which both provides efficient checks and minimizes the software TCB. To measure the performance of our scheme, we compartmentalized the IPv6 and NFTables kernel modules, and evaluated using Apache and by browsing the Alexa Top 50 websites. Here we provided the kernel source files with out annotations to define the compartments, as well as the LLVM compiler pass we use to add the required checks to enforce our scheme.

HAKCs Setup

HAKCs requires building our LLVM pass (contained in PMC-Pass/src) before compiling the kernel (contained in MTE-Kernel). The directions for building the pass are located in PMC-Pass/README.md. Once the pass is built, the kernel can be built. Directions for building the kernel are also included in PMC-Pass/README.md.

rpi-setup contains directions for running on a raspberry pi as described in the paper.

packet-filtering contains scripts used for the packet filtering experiments described in the paper.

scripts contains various utilities.

Disclaimer

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).