Automotive OSS Survey

Company Mentor
James Baker

Faculty Advisor
Prof. Nhut Nguyen

CS 4485 / Spring 2024
Department of Computer Science
Erik Jonsson School of Engineering & Computer Science
The University of Texas at Dallas
Richardson, TX 75080, USA

Alexandria Andrade
aaa210007
(@utdallas.edu)

Avinash Vadivelu
axv200086
(@utdallas.edu)

Lucas Noack
lan210002
(@utdallas.edu)

Michael Graves
mdg200001
(@utdallas.edu)

Ngoc Huynh
ngoc.huynh2
(@utdallas.edu)

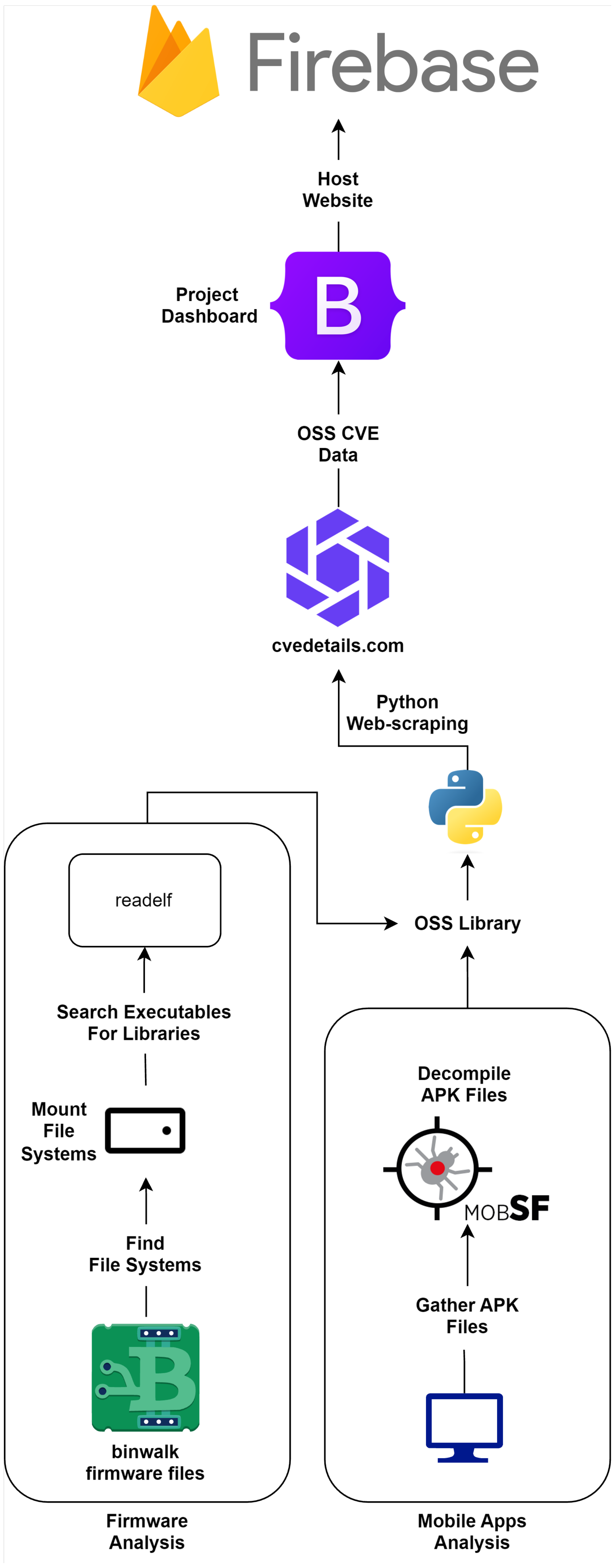
Ryan Gaulding
rsg200006
(@utdallas.edu)

Abstract

Toyota currently prioritizes staying innovative and competitive within the automobile industry as one of their top goals. Meanwhile, open-source software (OSS) is rapidly gaining popularity across many different industries, especially within the automobile industry. As the software-defined vehicle evolves, it is expected that the volume of software within vehicles will keep increasing, along with the presumed rise in the utilization of OSS. This project seeks to quantify the rise in automobile focused OSS by evaluating their security risks or advantages, quantifying their current and evolving adoption rates, identifying key OSS projects within the industry, and showcasing our findings on a web-based dashboard.

Keywords: Open Source, Automotive, Reverse Engineering, Firmware, Mobile Apps

Architecture



Project Dashboard
Holds our findings and gives a summary of each firmware and app we analyzed. It was coded with HTML/JS using Bootstrap 5.

Firebase
Hosts the project dashboard online so everyone can access it.

cvedetails.com
Provides the CVE data for each library that we inspect.

MobSF
Used to decompile Android APKs to find which libraries each app uses.

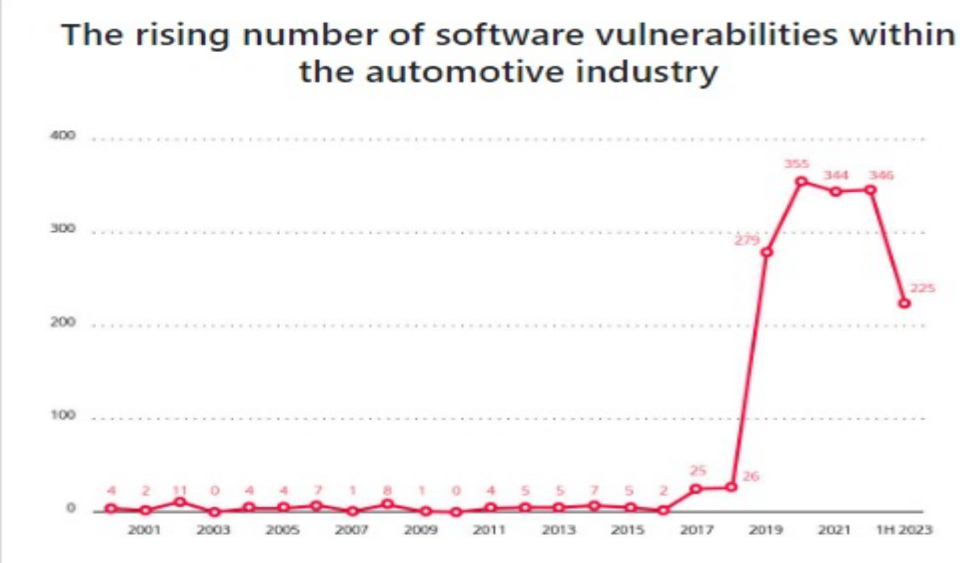
Binwalk/Readelf
Binwalk is used to analyze the automotive firmware. Readelf is used to find which libraries an executable file uses.

Metrics

- 4 Firmware files and 5 Mobile apps from the automotive industry were analyzed
- Hundreds of open-source libraries analyzed
- Thousands of CVE entries parsed and utilized
- Over 10 libraries found which are automotive specific and not general-purpose
- 13 different web pages created for the dashboard
- We completed 100% of our core requirements

Impact

- Our project's findings on the prevalence of open source in the automotive industry will profoundly influence Toyota's future firmware and mobile software development endeavors, reshaping their future strategies in regards to firmware.
- With the Common Vulnerabilities and Exposures (CVEs) found from our open source research, Toyota will have valuable knowledge that will enhance their future software development initiatives, particularly in fortifying the security aspects of their embedded software systems.



Credit to TrendMicro for the graph.

Summary

Our team reverse engineered different firmware files and mobile apps to uncover various OSS used within them. We utilized low-level tools such as Binwalk and Readelf to reverse engineer and delve deeper into the analysis of firmware files. Similarly, for the mobile apps, MobSF along with various Linux commands were utilized. The CVE data for each library was compiled onto a project dashboard with the use of Python scripts. This dashboard hosts all the OSS we found, their CVEs, and key findings within the firmware and mobile apps. Our work has allowed Toyota to have a better understanding of the usage of OSS within the automotive industry and better asses the risk associated with the increasing adoption of it.