Sdmay21-41

Vincent Johnson - Team Lead: vincentj@iastate.edu
Joshua French
Jordan McKillip
Marcus Reecy

IoT Security Verification

The Internet of Things (IoT) is becoming more and more a part of people's everyday lives. Devices such as locks, cameras, and smart-speakers are just a very small view of all the ways our lives are going online. With all of these devices having important roles, being located in private places, and gathering loads of information, the security of them is much more prevalent as it would be problematic if it got into the wrong hands.
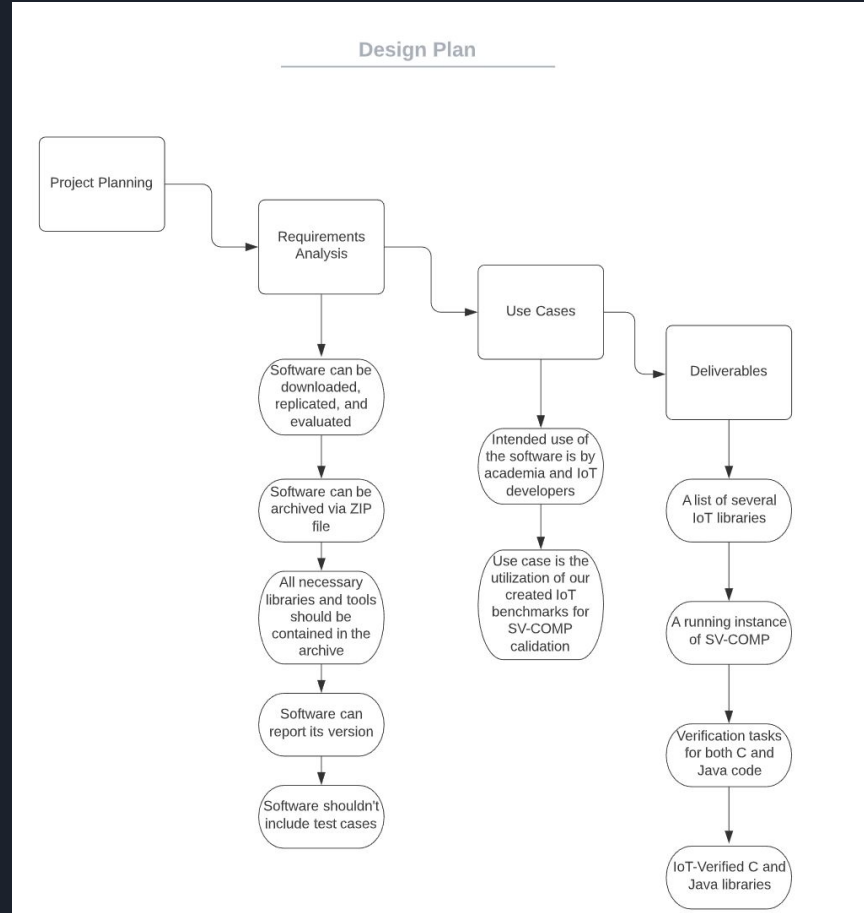
Overall Goal

The overall goal of the team is to validate IoT Source Code and/or Libraries with validation tasks using our defined security properties, modified IoT source code, and tools provided by SV-COMP.

From our validated validation runs we will then set IoT benchmarks for others to use to test code with their own validation tasks.
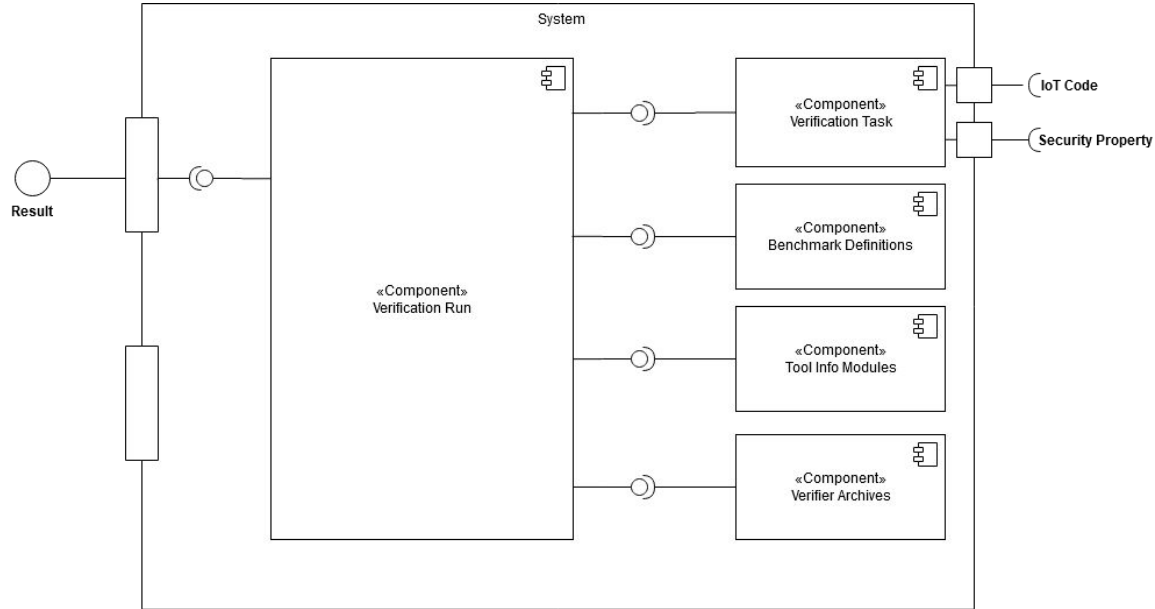
Design Plan

Use Case Diagram
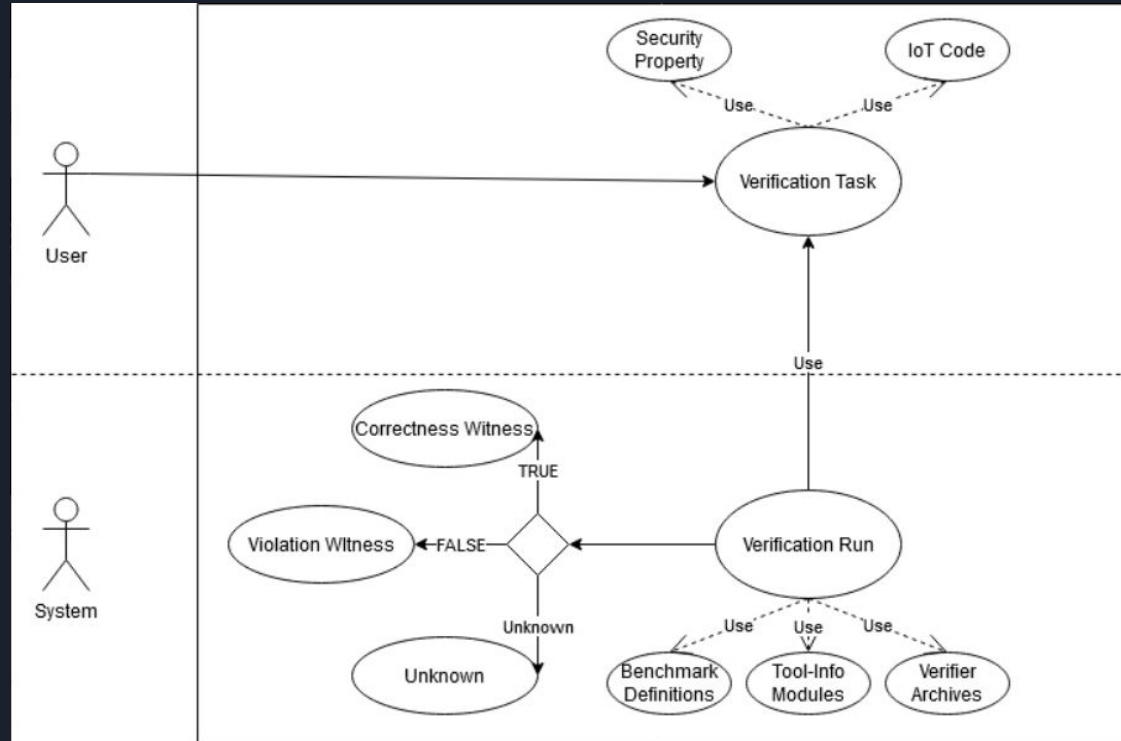
Benchmark Component Diagram

Definitions:

- Benchmark - a file that specifies the files and properties that the tool must test. This also acts as a configuration file.
- LTL Formula - the formula that specifies states and/or conditions that the program must meet
- Model Checking - a method of checking whether the system meets the given specification
- Verification Task - a verification task consists of a C/Java program and a security property
- Verification Run - a non-interactive execution of a tool on a single verification task
  - Correct True - The specification was satisfied, the expected correct value was produced by the tool
  - Correct False - The specification was violated, the expected false value was produced by the tool
  - Unknown - The tool cannot determine the answer - the tool terminates by crash, time-out or ran out of memory.

Technical Challenges

- VM issues
  - Access
  - Kernel
  - Memory
- Understanding the system
- Tools running custom security properties