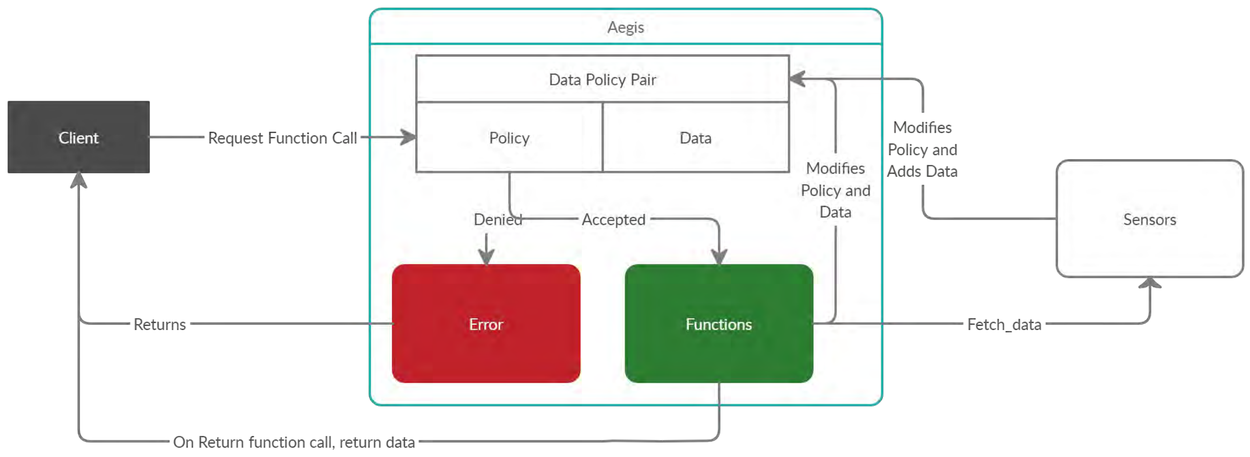
Vassar College | Undergraduate Research Summer Institute (URSI) Symposium | 2020

Aegis: A Smartphone Data Privacy Solution

Nicholas Weiner ‘22, Jemma Brooker ‘23, Ryan Hornby ‘21
Faculty Advisor: Jason Waterman

Special thanks to: URSI Faculty and Student, Vassar College



INTRODUCTION

Just by existing, our smartphones generate and collect large amounts of data. This collection of data can be used to provide us with useful services, like video recommendations, navigation software, and accurate local weather forecasts. Unfortunately some companies are not clear with their intentions. One such intention is to sell your data to advertisers. With Aegis we aim to allow the user to decide how they want their data to be used, rather than the application.

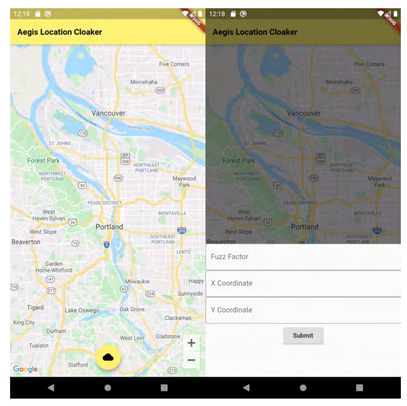
METHODOLOGY

- **Aegis is a run-time monitor of iOS and Android applications**
- **It is an intermediary between a client app and the sensors that generate sensitive data.**
- **It is a Flutter plugin, allowing cross-platform development.**
  - **Aegis only accepts function calls for sensitive data that are explicitly whitelisted in the plugin.**
- **The Aegis protocol was modeled on Ancile, a similar framework for protecting sensitive data on non-mobile applications.**

DATA POLICY PAIRS

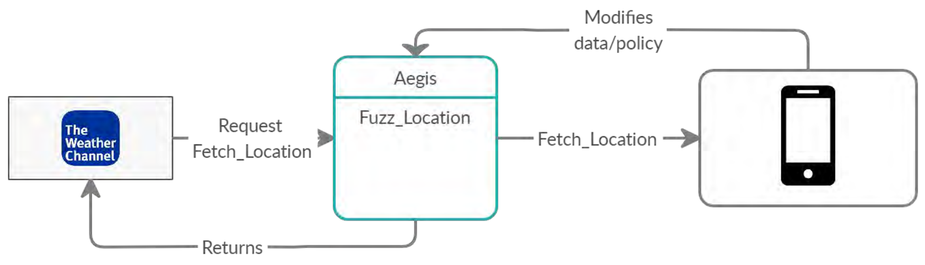
The essential building blocks of Aegis are objects called Data Policy pairs. Each Data Policy pair contains a dictionary which represents the data and a regular expression which contains the privacy policy language. A regular expression is a grammar which computers can reason with. It is impossible to split the data from the policy without the policy’s permission. Any operations performed by Aegis modifies both the data and the policy.

IMPLEMENTATION



THE AEGIS LOCATION ANONYMIZER

The Aegis Location Anonymizer takes input of two coordinates and a “fuzz factor” (the degree to which the user wants their location anonymized), and displays the radius boundaries within which the user is located; what Aegis would then be showing to any outside apps.



A LESS INVASIVE WEATHER APP

IBM’s “The Weather Channel” app is a prime example of an app that abuses its access to sensitive data; the app sells collected location data to advertisers. Aegis solves this problem by allowing the anonymization of location data, as shown above. Weather apps do not need exact locations; an approximation is enough to give accurate weather results, providing the weather service while protecting users’ privacy.

FUTURE WORK

In the future, Aegis will be developed into an app, published on the Google Play & Apple IOS app stores. We hope to make the app more secure. The app will be built from the current library and function locally, on the phone, communicating with other apps. Aegis’ functionality is displayed in an app we developed to anonymize location to within a particular radius boundary.

UNDERGRADUATE RESEARCH SUMMER INSTITUTE
Est. 1986 at Vassar College

VASSAR COLLEGE · A.D. 1861 ·