

**CHENNAI – PONDICHERRY**

**Characterizing Privacy Risks of Mobile Apps with Sensitivity Analysis**

**Abstract:**

Given the emerging concerns over app privacy-related risks, major app distribution providers (e.g., Microsoft) have been exploring approaches to help end users to make informed decision before installation. This is different from existing approaches of simply trusting users to make the right decision. We build on the direction of risk rating as the way to communicate app-specific privacy risks to end users. To this end, we propose to use sensitivity analysis to infer whether an app requests sensitive on-device resources/data that are not required for its expected functionality. Our system, Privet, addresses challenges in efficiently achieving test coverage and automated privacy risk assessment. Finally, we evaluate Privet with 1,000 Android apps released in the wild.

**Existing System:**

The problem of risk rating can be reformulated as the proven sensitivity analysis, or an iterative process that substitutes alternative input parameter values to measure changes in output values. In the case of mobile apps, we want to determine if app outputs (i.e., user-perceived app functionality) change with different app inputs (i.e., privacy settings for an on-device resource/data). Such cases would suggest the app functionality has a high probability of dependence on the corresponding resource, and hence a lower risk rating. We note that this article focuses on sensitive on-device data, as full analysis on the closed app backend is typically not possible.

**Proposed System:**

We present a novel concept of applying sensitivity analysis to assess an app’s privacy risks, by considering whether a requested sensitive resource would contribute to any user-perceivable app features. Then, we systematically implemented this concept as Privet, and we evaluated with top 1,000 Android apps (from Google Play) over 10 categories of sensitive data.

We found that more than 48.7% of apps can have at least one type of resource requests blocked or manipulated, without impacting user perceptions. For example, the lack of home addresses from the address book does not prevent most social networking from recommending friends. Moreover, the system scalability is practical for real-world testing – compared to the standard practice of random automation, targeted app automation can achieve the same testing coverage, with an average of 85.3% less testing time. Finally, the automated assessment can achieve a classification accuracy of 93.4%, as evaluated against human labels.