**TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring (S01)**

Many of today’s smartphone operating systems fail to monitor, control, and report the use of personal data by third-party applications. TaintDroid aims to create an efficient, system-wide tracker that provides real-time monitoring of multiple sources of sensitive data by leveraging Android’s virtualized execution environment. In order to sustain real-time monitoring in the wild, several challenges must be addressed: (i) constrained smartphone resources, (ii) dynamic sensitive information, and (iii) shared information between applications. These issues are resolved by using a multi-granular approach that marks sensitive information at the variable-level (within application code), message-level (between applications), method-level (within native libraries), and file-level (within storage). When deployed on 30 popular applications, TaintDroid found that approximately one third of applications expose device ID, and half share location data, all the while generated no false positives and minimal latency while running.

**Location Privacy in Pervasive Computing (S02)**

With location-aware applications becoming more and more ubiquitous, we need to address the problem of protecting our location privacy. However, it needs to be said that location-aware applications are definitely useful - so the challenge is to control our location privacy without restricting it. The authors introduce the mix zone, which is a privacy-protecting framework based on frequency changing pseudonyms so users can avoid being identified by the locations they visit. Because applications share information with each other, the authors also recommend using different pseudonyms for different applications. When applied to the authors’ Active Bat system, the temporal and spatial resolution of location data is too high to keep location private, but the authors expect to have a higher degree of unlinkability between pseudonyms over a larger, more populated area.

**User-Generated Free-Form Gestures for Authentication: Security and Memorability (S04)**

Smartphones and tablets are important for secure daily transactions, such as email access, mobile payments, or even access to homes - which makes ensuring the security of our mobile devices of paramount importance. The authors study the security and memorability of freeform multi-touch gestures as a means for mobile authentication. The main challenge is creating a metric to analyze security of these free-form gestures. To do so, the authors introduce a novel metric based on computing the estimated mutual information of repeated gestures, and studied the performance against shoulder surfing attacks. Using a generate-test-retest ideology, the authors estimated that security is relatively high for most free-form gesture passwords created. Interestingly, multi-finger gestures do not show high security with this metric, which can be attributed to most multi-finger gestures as merely repeating the same single-finger gesture with multiple fingers.

**Matthan: Drone Presence Detection by Identifying Physical Signatures (S07)**

With the advent of inexpensive, commercially available drones, there comes an increased presence of drones flying in sensitive airspace where their presence can be harmful. Therefore, a need to create a cost-effective detection system is required to warn the presence of drones in these cases. The authors introduce Matthan, a system for detecting drones by identifying unique signatures of a drone’s body vibration and body shifting in the Wifi signal transmitted by the drone. A big challenge is being able to differentiate drones from other mobile wireless devices. To this end, Matthan uses a joint detector that uses both a frequency based detector as well as a wavelet-based detector to calculate the drone’s vibration and body shifts. When tested in three real-world environments with SDR radios and seven different drones, Matthan was capable of detecting drones with an accuracy of above 90% at 50 meters, and 80-85% at 600 meters.

*The security and privacy area honestly shocked me due to how easy it is for applications to secure and send sensitive data. It makes me hopeful that there are many smart people who are actively working on looking for solutions to protect the privacy of the average consumer, and makes me enthusiastic about what I can do to help contribute to this cause.*