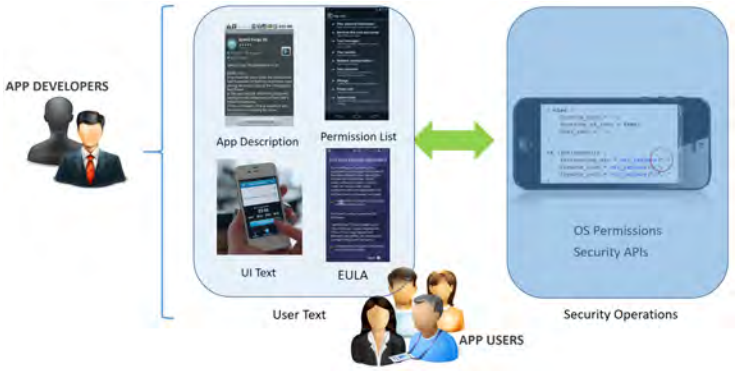
# TWC: Medium: Collaborative: Improving Mobile-Application Security via Text Analytics

**Challenge:**

- Security and privacy analysis of mobile applications is insensitive to the end-user's expectations of the application's runtime behavior, which negatively impacts both the soundness and completeness of those analyses.

*How can security decisions be improved by using **expectation context** inferred from textual artifacts?*




*Our results demonstrate novel techniques to establish relationships between user text and security operations.*

**Solution:**

- We have studied the existence of grayware on the Google Play store via text analytics.
- We have investigated text analytics to identify questionable apps based on app store metadata.
- We have investigated usefulness of NL text in application user interfaces as it pertains to security and privacy sensitive operations.

**Scientific Impact:**

- We have studied outliers in mobile app requests for security/privacy sensitive user input.
- We have found that text analytics is useful for studying mobile grayware.

## Broader Impact:

- The results impact the future design of computing platforms such as Android, iOS, and Windows.
- Project artifacts such as mobile grayware dataset and results have been made publically available.
- PI Xie has engaged extensively with members from U. Illinois NSBE chapter on raising the awareness of mobile security.


CNS-1513939

PI: Tao Xie, Co-PIs: Carl Gunter, ChengXiang Zhai (U. Illinois) {taoxie,cgunter,czhai}@illinois.edu

CNS-1513690

PI: William Enck (North Carolina State U.) whenck@ncsu.edu