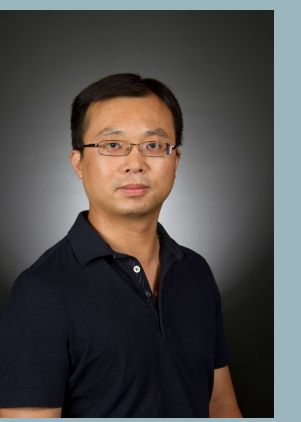# TWC: Small: Secure Mobile Devices through Multiple Lines of Defense

PI: Yanchao Zhang, Arizona State University

The objective of this project is to develop secure and usable countermeasures against new attacks when mobile devices are watched, or intruded, or lost/stolen.

- A study reveals that one laptop is stolen every 53 seconds; 70 million smartphones are lost every year, with only 7% recovered; and 4.3% of company-issued smartphones are lost/ stolen every year.

- There were as many Android devices infected with malware as Windows laptops in the second half of 2014 alone.

- Existing techniques cannot defend against the attacks studied in this project.

- There is a pressing need to develop more thorough protection mechanisms.
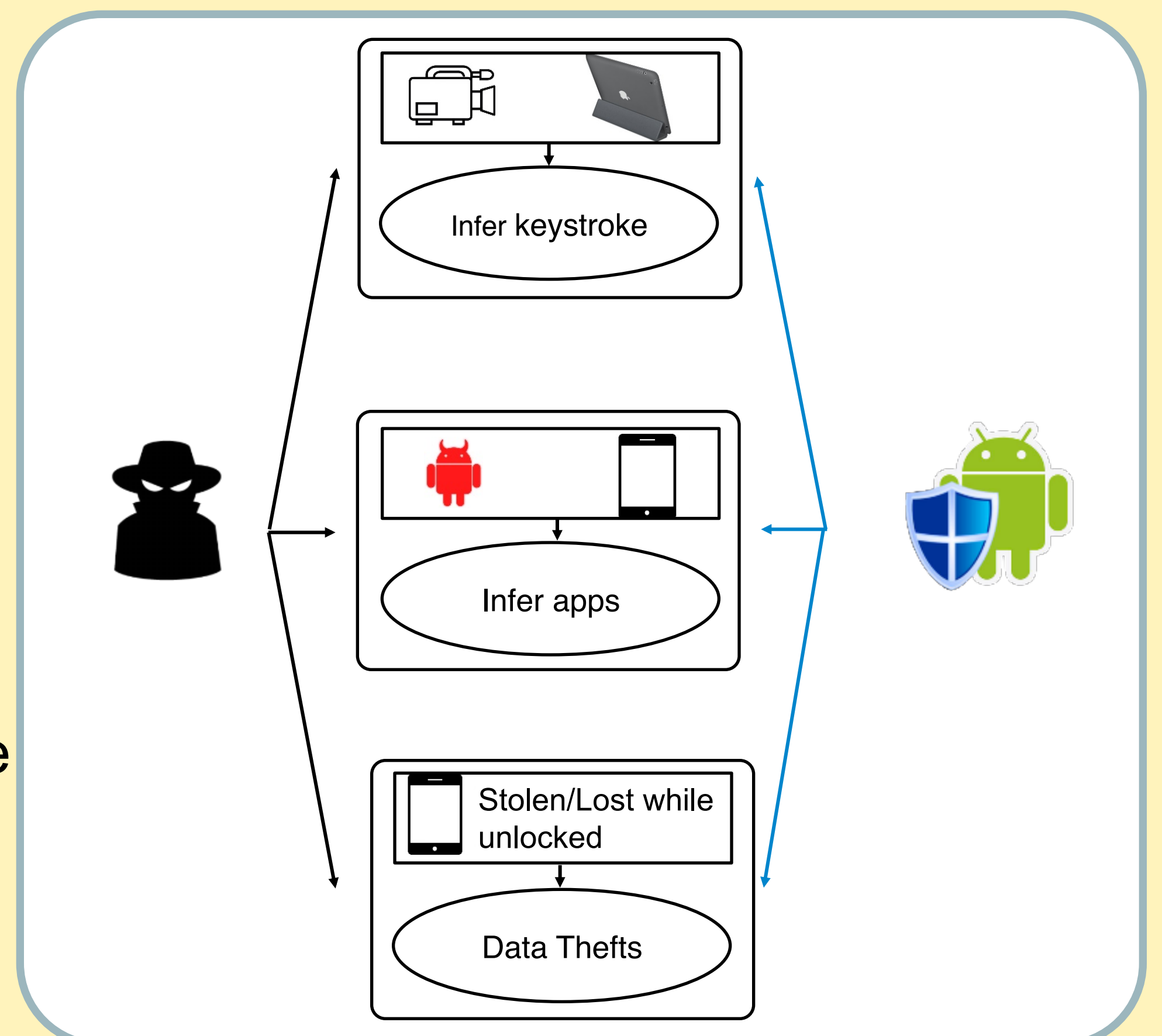

Approach

- Different keystrokes on tablets create different motions, identified by amplifying motions of the backside of a tablet.

- Different apps on mobile devices create different power profiles, recognized by building a machine-learning-based classifier.

- User departure can be detected by active acoustic signal sensing. Devices can immediately and automatically lock themselves upon user departure.

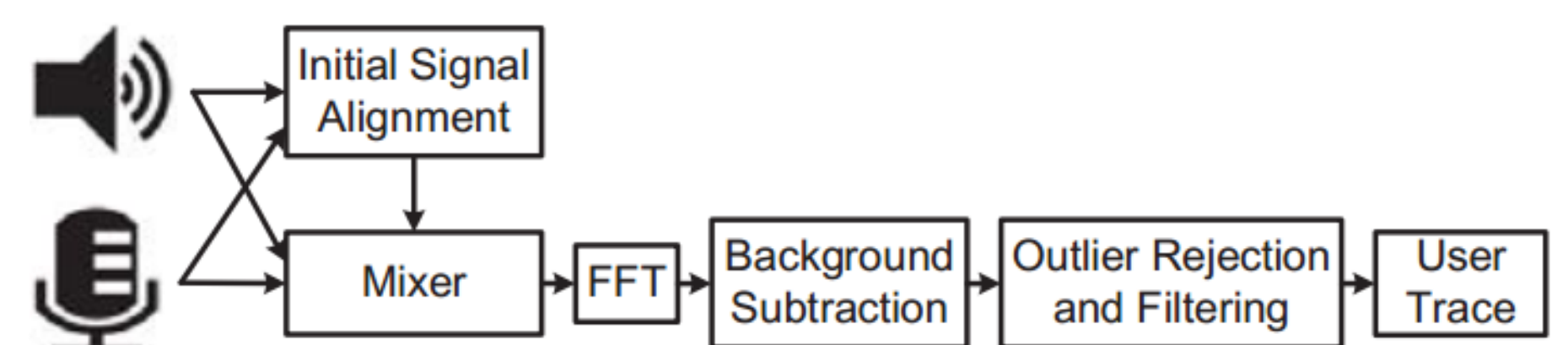### Mobile application fingerprinting

- Fingerprint an app by analyzing the power profile of the device.
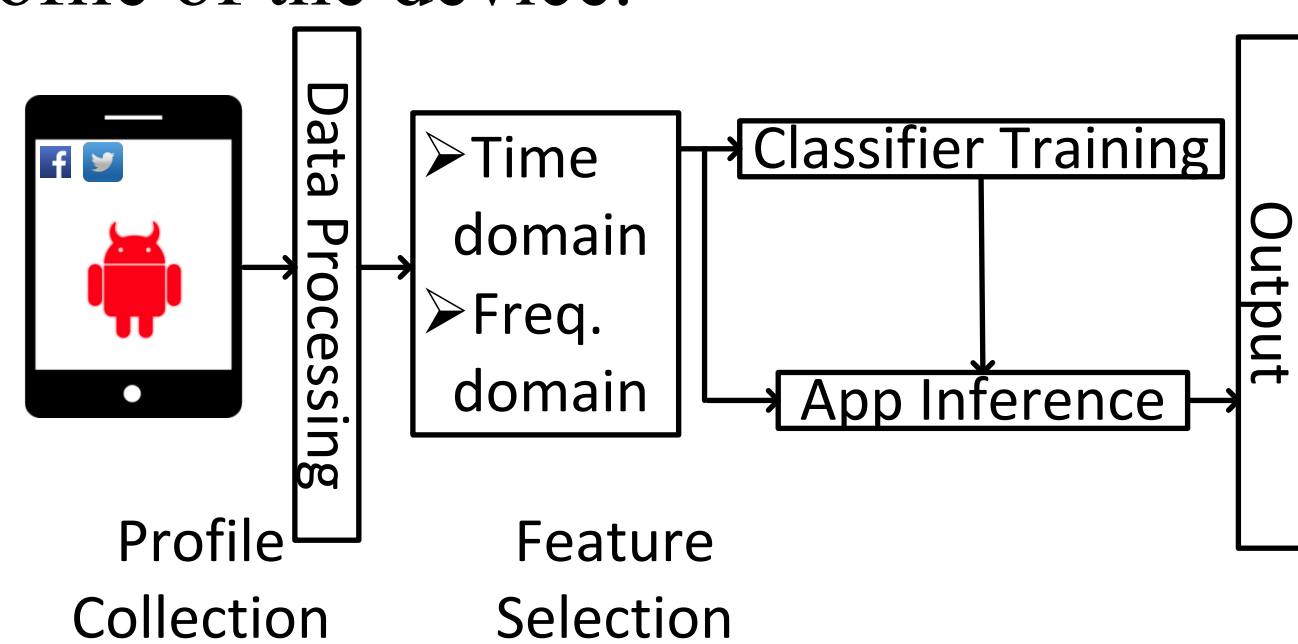
"POWERFUL: Mobile App Fingerprinting via Power Analysis", INFOCOM'17

Continuous authentication

- Detect user departure from the change in acoustic signal.

"iLock: Immediate and Automatic Locking of Mobile Devices against Data Theft", CCS'16

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN