Introduction & Motivation
• Smart wearable devices, such as smartwatches, are becoming mainstream and fast replacing their traditional non-smart counterparts.
• However, there is inadequate understanding and awareness of the various side-channel security vulnerabilities that are enabled by these wearable devices, and how to protect users against them.

Side-Channel Attacks
We demonstrate that wearable devices enable novel side-channel security and privacy threats:
• Mobile keystroke inference [1,6]: Key tap inference attacks on handheld numeric touchpads by using zero-permission smartwatch motion sensors as a side-channel.

• External Keyboard keystroke inference [2]: Keystroke inference attacks on external QWERTY keyboards using smartwatch motion sensors as side-channel. We characterize wrist movements based on the relative physical position of keys and the direction of transition between pairs of keys. Keystroke characteristics are then matched to candidate dictionary words.

• Location tracking (in progress): Tracking automobile drivers using inertial information computed from driver’s smartwatch.

Evaluation Results
• Mobile keystroke inference:
Experimental evaluation using commercial off-the-shelf smartwatches show that key tap inference using smartwatch motion sensors is not only fairly accurate (more than 90% in certain scenarios), but also comparable to (and better than) similar attacks using smartphone motion sensors.

• External Keyboard keystroke inference:

Protection Measures
We developed design-time and run-time protection mechanisms to protect against some of the demonstrated side-channel attacks, while preserving acceptable usability/utility of the wearable devices:
• Context-aware sensor access control [2]: Untrusted applications get access to motion sensors only when rTAD reports that the user is not typing at the moment.

• Randomized mobile keypads [3] and augmented reality keyboards [4]:

• Studying and increasing security awareness among users [5].

Publications Till Date