Pseudo-\(\epsilon\)-Differential Privacy for The \textit{Posturizer}

An Exploration into Privacy Mechanisms with a Custom Posture Monitoring Device

Michael Ostertag
CSE 237A
Winter 2016
The Three-Fold Motivation

1) Develop a sensing platform for posture monitoring
   • Growing problem in an increasingly sedentary world
   • Quantified self movement is a market hungry for new products

2) Utilize platform to experiment with low-computational privacy
   • By 2020, 50 billion integrated smart devices with privacy concerns, many will be resource-constrained devices

3) Design and build an embedded system from ground up
   • Project increased my coding expertise from “sparse” to “fair”
Inventive Hardware Design (Prototype)

**Arduino Pro Mini**
- Microcontroller
- 8 MHz Clock
- 32 KB Program
- 1 KB NVM
- Plenty of IO

**ADXL362**
- 3-Axis Accelerometer
- Low Power
- SPI Communication
- Interrupt for Activity/Inactivity

**Push Button**
- OFF-MOM

**Status LEDs**
- Debugging and State Tracking
- Low current configuration

**9 V Battery**
- Battery...
- ... at 9 V

**Active Buzzer**
- DC powered
- Obnoxious at 5 V
Pseudo-$\epsilon$-Differential Privacy

- **Goal:** Control the amount of information third-party learns from data by adding noise to obscure identifying features.

- **Privacy Mechanism:** $\epsilon$-Differential Privacy by Dwork [2002]
  - Exponential distribution ($\mu = $ true data point, $\sigma = \Delta f / \epsilon$, where $\epsilon$ sets the desired privacy level and assuming $\Delta f = 1$ activity level change)
  - ‘Pseudo’ due to bounding between [0, 6] and normalizing, allowing creation of lookup tables for 8 fractional bits but introducing biasing
  - Probability distributions for varying $\epsilon$. Colors represent different input values.
Amazing Results

- User-selectable Privacy:
  - None (1.0), Low (0.9), Medium (0.5), or High (0.1)

- Low-cost Implementation:
  - 8 MHz, single core microcontroller

- Robust when republishing:
  - Same random number seed for each recording session/privacy level combination.

- Results from experiment -->
  - 4 min stationary, 4 min moving, repeated