CPS: Breakthrough: Secure interactions with Internet of Things (CNS-1646130)

Kang G. Shin
CSE/EECS, University of Michigan

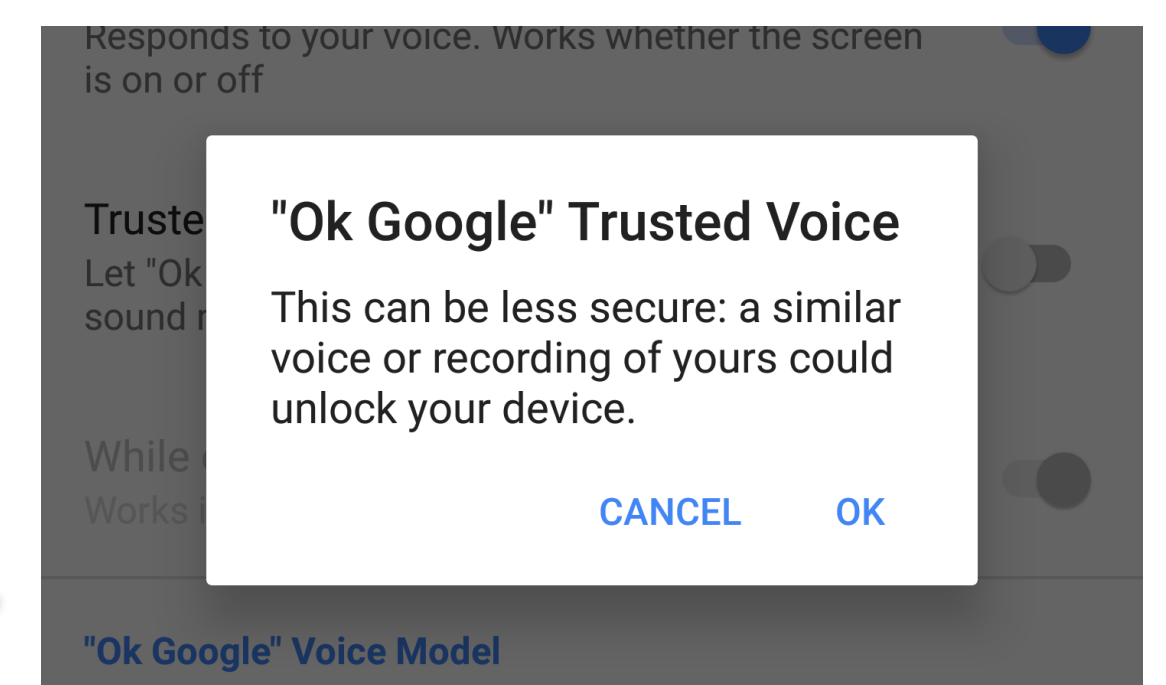## 1. Motivation

1.1 Voice – An Emerging Interaction

Voice assistant is a popular interaction channel with IoT devices

We need to **secure** the voice channel!

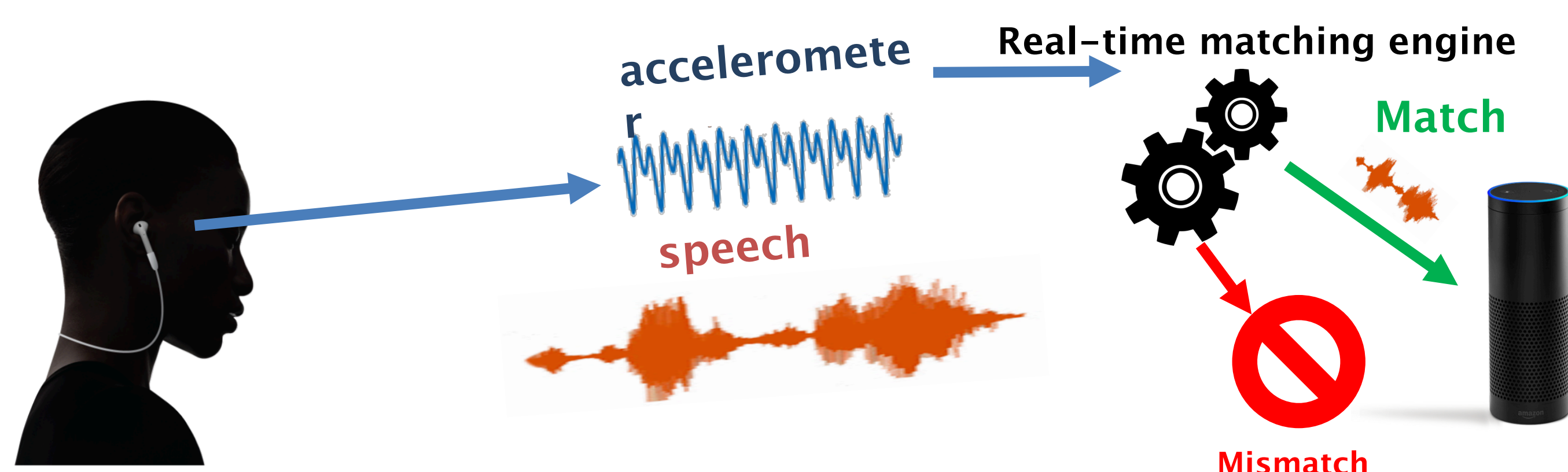### 1.2 Limitations of Voice Assistant

Voice assistants listen to everyone (thing)

1.3 Why Not Voice Biometrics?

"Ok Google" Trusted Voice

This can be less secure: a similar voice or recording of yours could unlock your device.

CANCEL   OK

"Ok Google" Voice Model

Voice biometrics cannot be trusted!

2. System Design

2.1 VAuth – Continuous Voice Authentication

accelerometer

Real–time matching engine
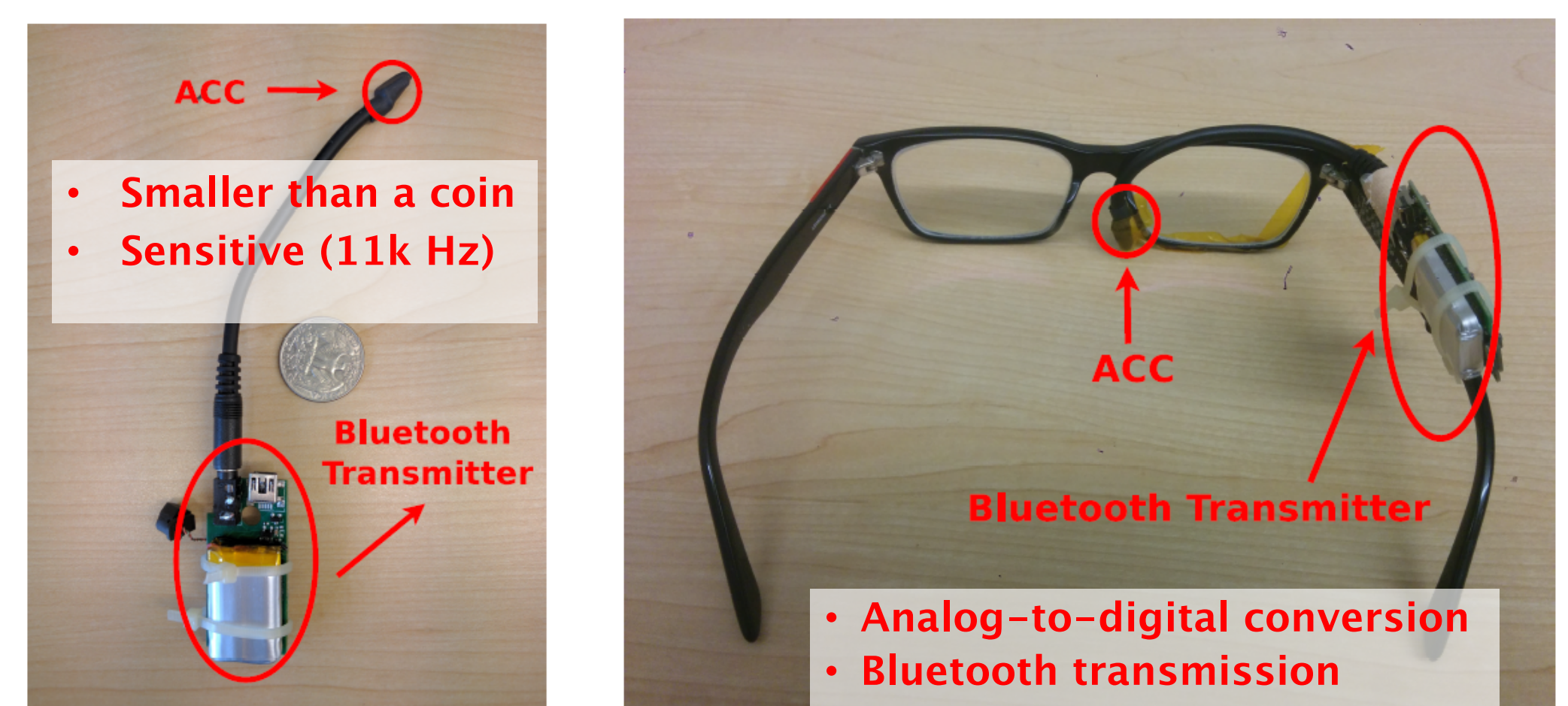
Match

speech

Mismatch

2.2 Matching Algorithm

- Pre-processing
    - High-pass filter -> Re-sample -> Normalization
    - Keep segments that match human speech

- SVM-based decision making
    - Feature: the vector of cross-correlation
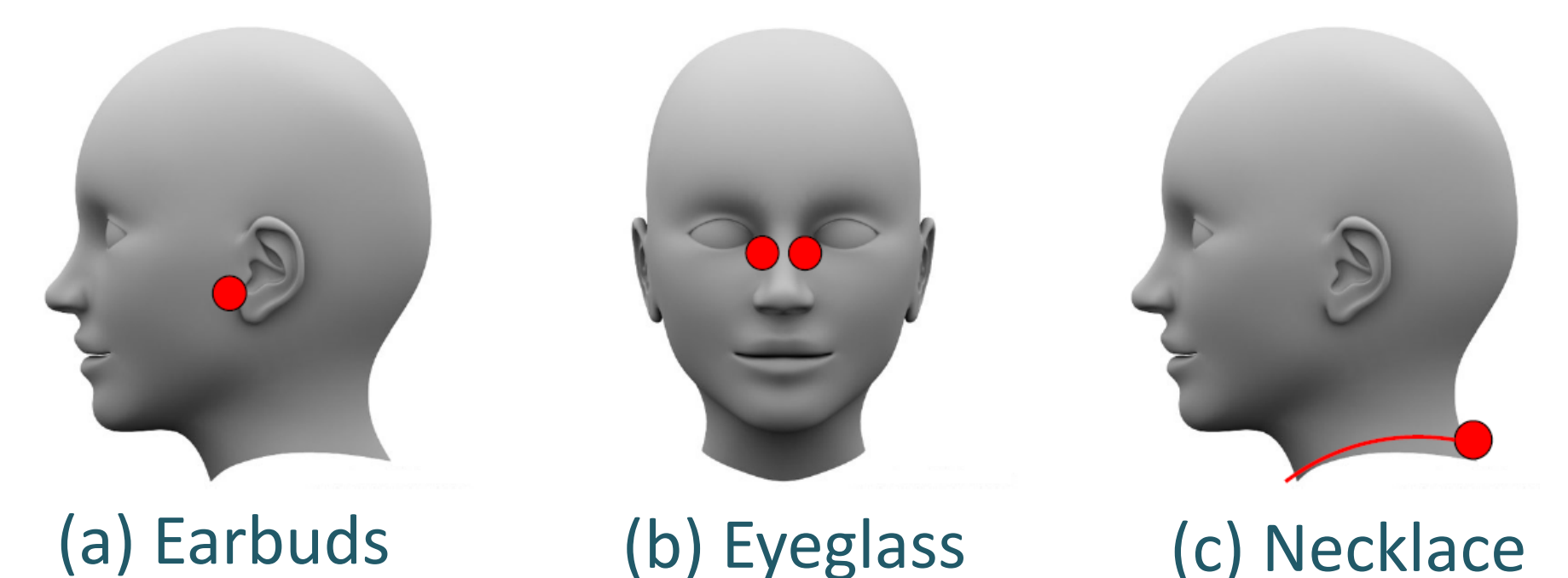   - Training set: One user on all 44 English phonemes
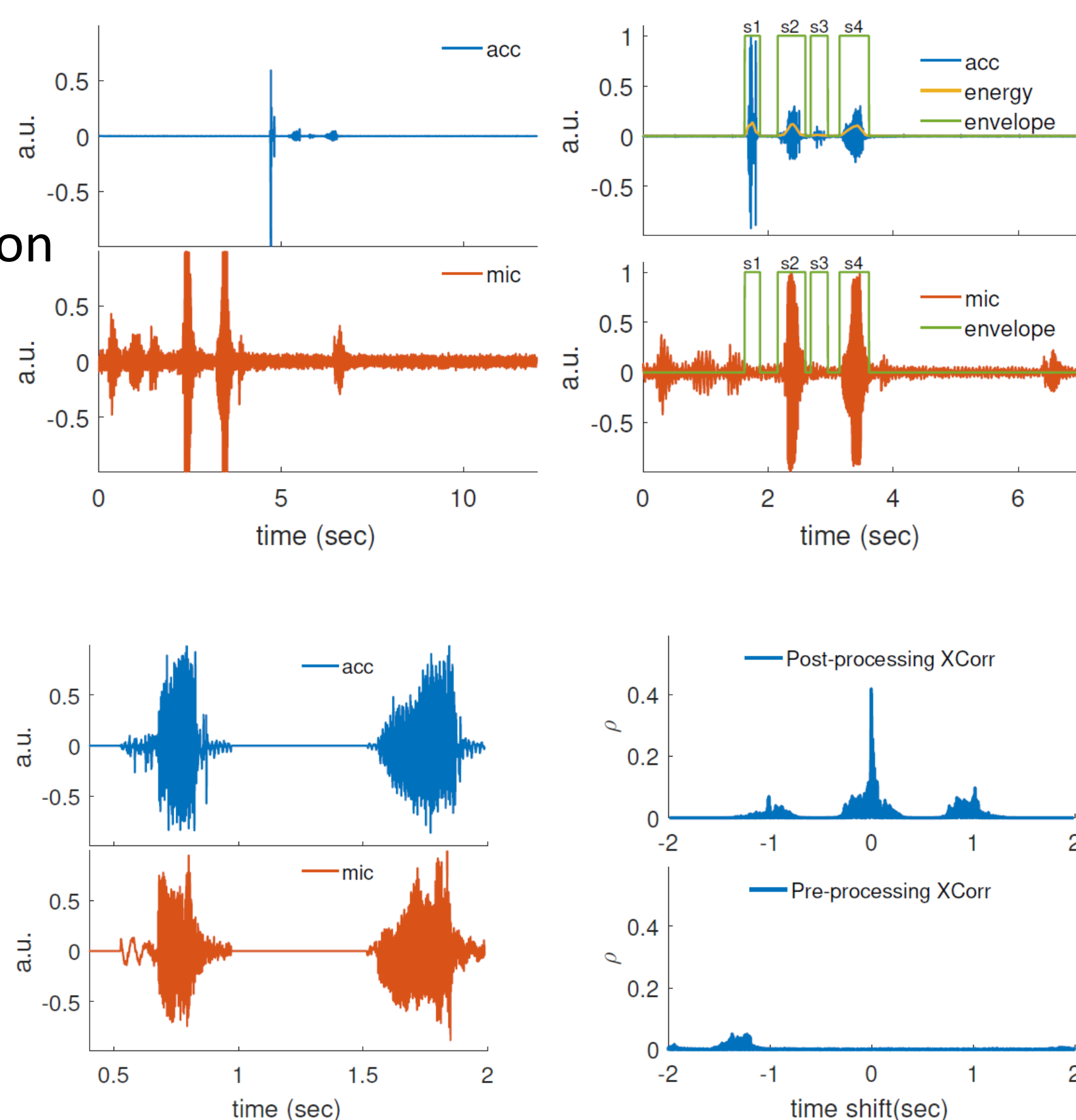
3. Hardware & Usability

3.1 Wearable component

- ACC
- Smaller than a coin
- Sensitive (11k Hz)
- Bluetooth Transmitter

- ACC
- Bluetooth Transmitter
- Analog–to-digital conversion
- Bluetooth transmission

3.2 Usability

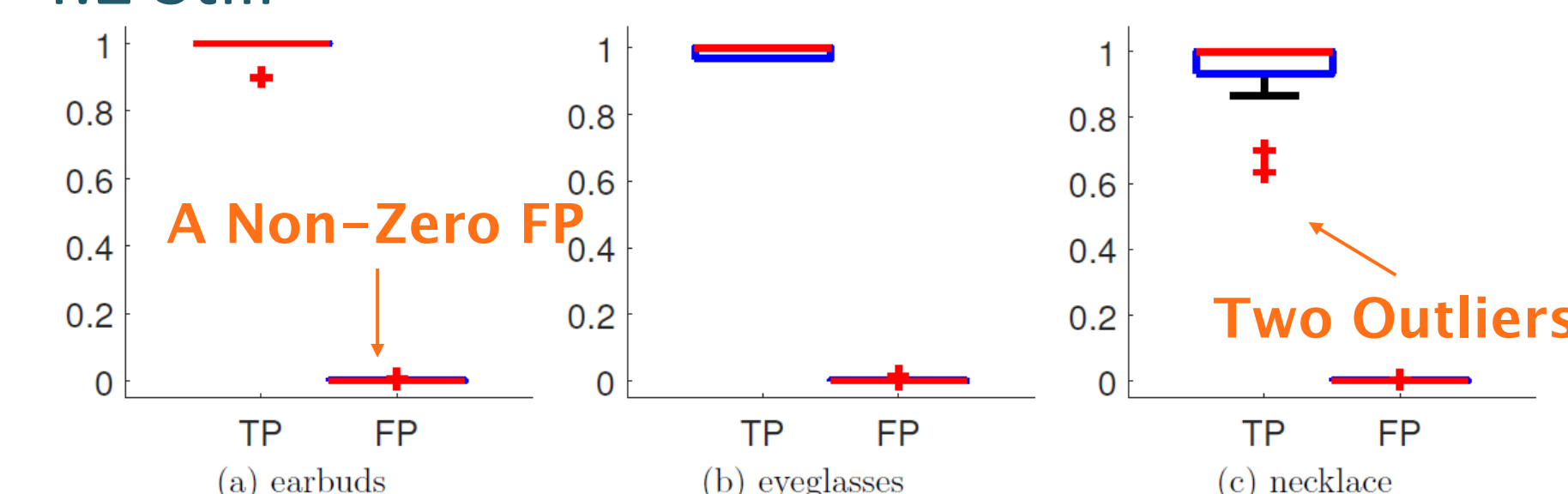(a) Earbuds   (b) Eyeglass   (c) Necklace

- Reusing wearables that are already being used everyday
    - Wear an additional device for security
    - Embed VAuth in existing wearable products
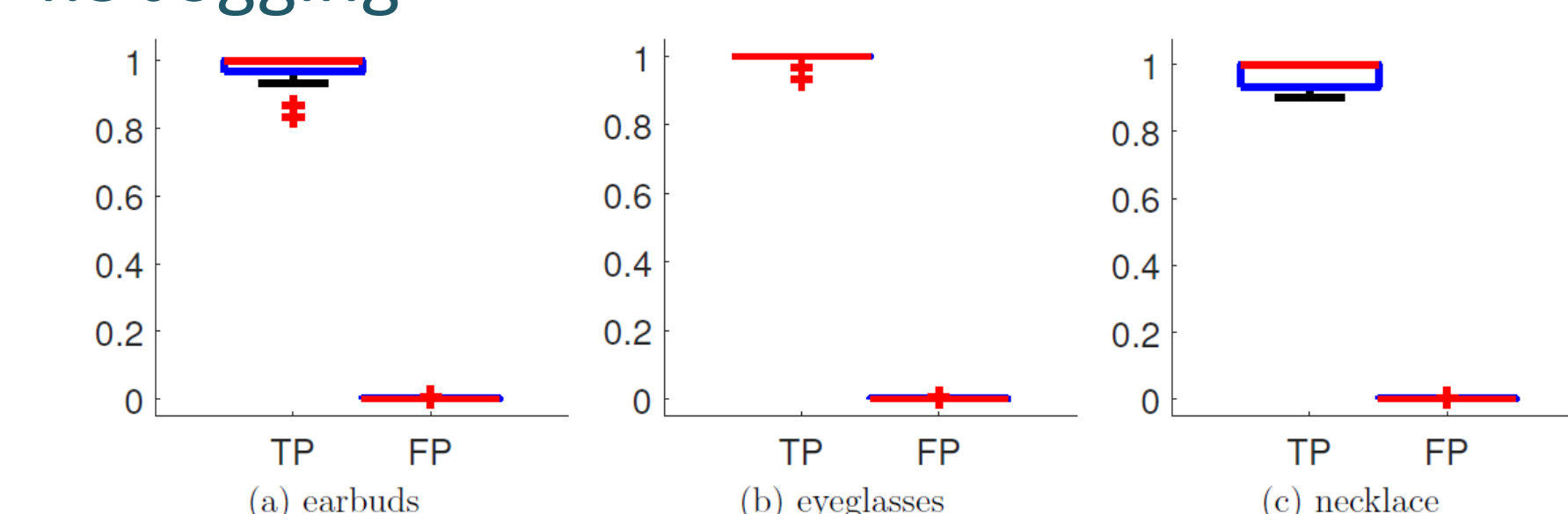
4. Evaluation

4.1 Settings

- Matching accuracy (true positive & false positives)
- **18** users speaking **30** commands under **6** scenarios
    - Three positions (eyeglasses, earbuds, necklace)
    - Two mobility patterns (still and jogging)
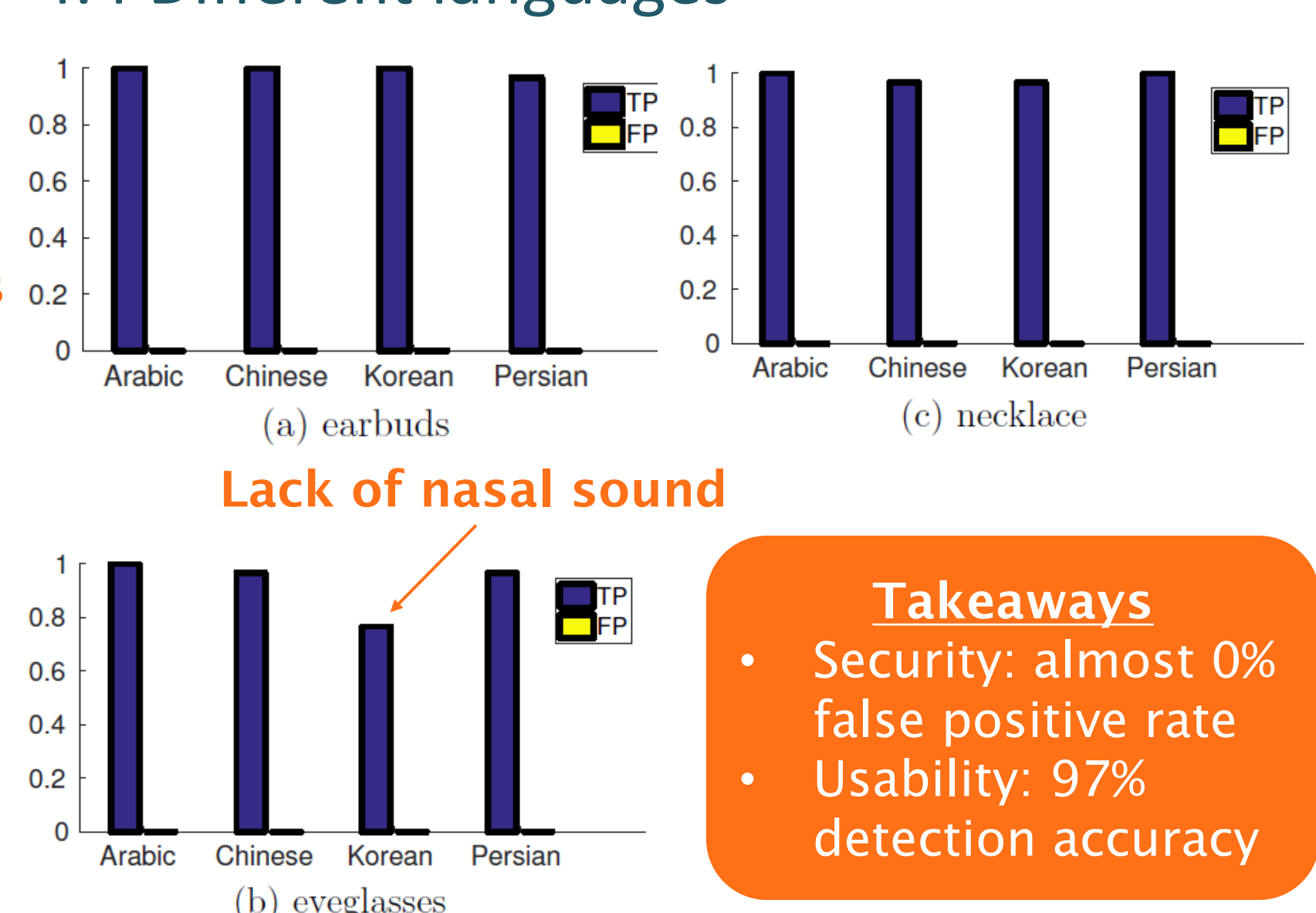   - 5 languages: English, Arabic, Chinese, Korean, Persian

4.2 Still

A Non–Zero FP

Two Outliers

(a) earbuds   (b) eyeglasses   (c) necklace

4.3 Jogging

(a) earbuds   (b) eyeglasses   (c) necklace

4.4 Different languages

TP / FP

(a) earbuds   (c) necklace

Lack of nasal sound

Arabic Chinese Korean Persian
(b) eyeglasses

Takeaways
- Security: almost 0% false positive rate
- Usability: 97% detection accuracy