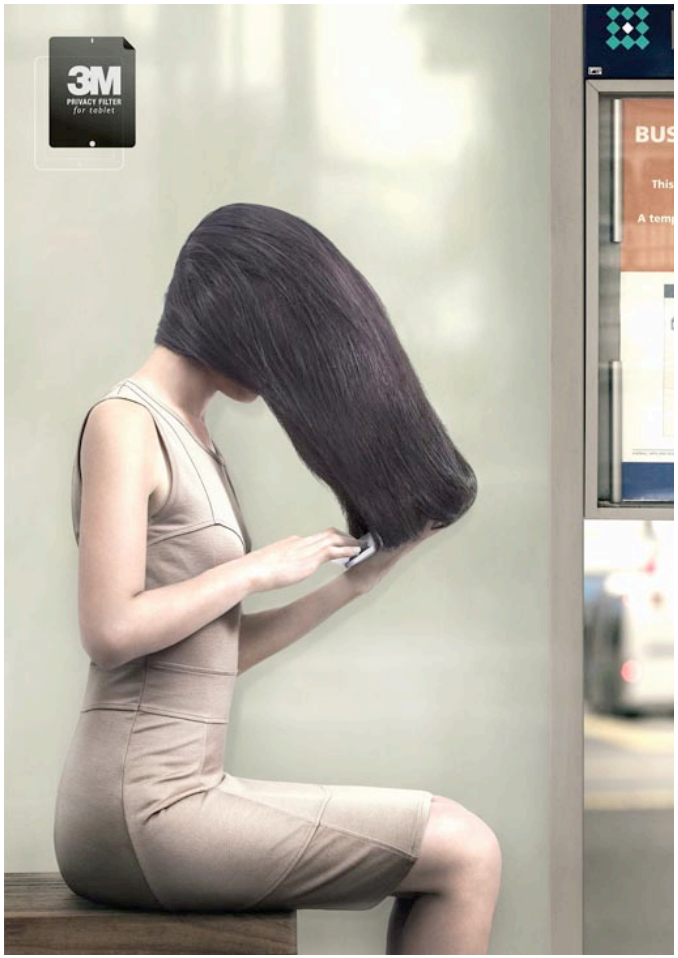
Imperfections of Sensors Make Smartphone Users Trackable

Wenyuan Xu

UNIVERSITY OF SOUTH CAROLINA

wyxu@zju.edu.cn

Privacy is not a new concern



Source: 3M privacy filter for laptops promotional campaign

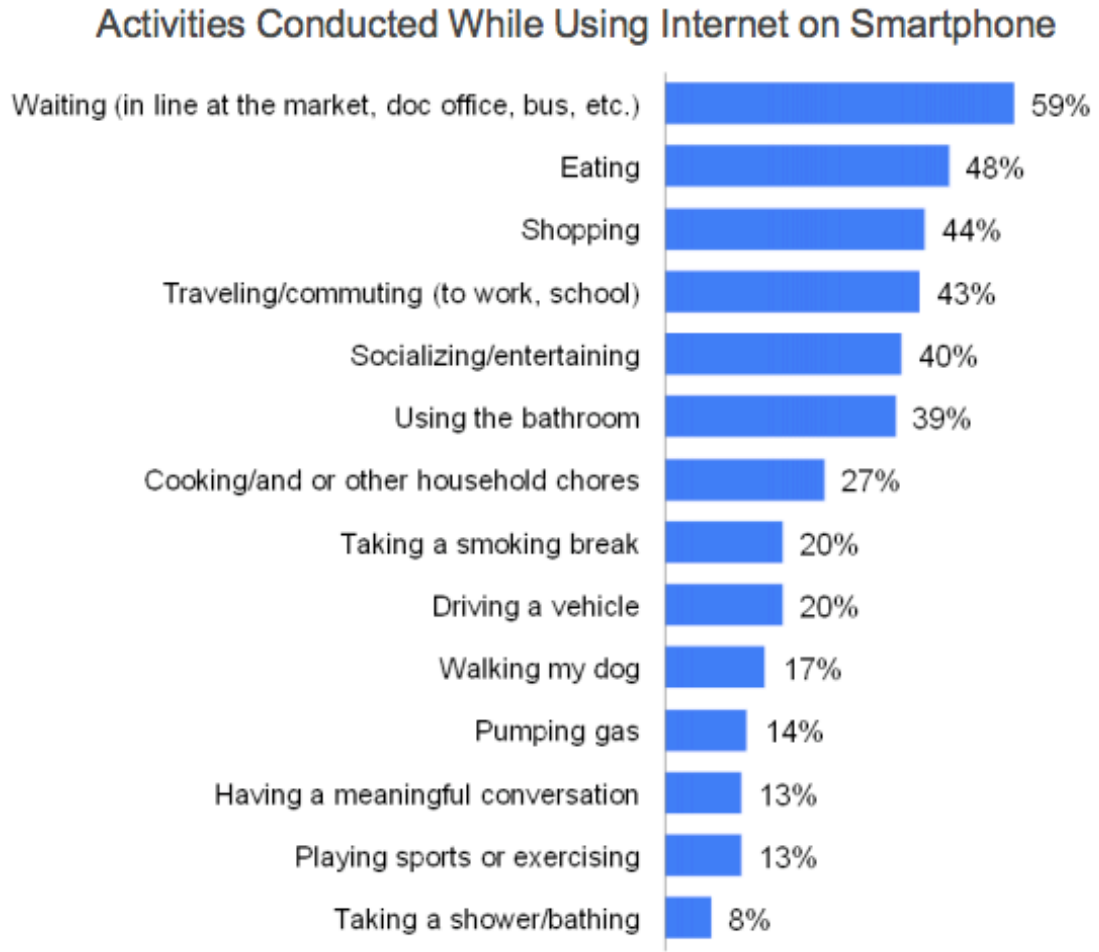
Smartphones are used everywhere

59%
Waiting in line

40%
Socializing

39%
Using the bathroom

27%
Cooking



Source: The Mobile Movement Study, Google/Ipsos OTX MediaCT , Apr 2011
Base: Smartphone Users (5013).
Q. Which of the following things would you be willing to give up for an entire month, in exchange for continuing to use the Internet on your smartphone?

A Closer Look at Smartphones

- Today, smartphones come with a wide range of sensors. All of which are useful for a variety of tasks.

accelerometer
gyroscope
magnetometer
front and rear cameras
NFC
barometer
speaker
microphone
proximity
light sensor
Bluetooth
GPS
WiFi + cellular
humidity
temperature

- Motion detection
- Gesture detection
- Audio Genre detection
- Location detection
- Interaction with nearby devices
- Compass

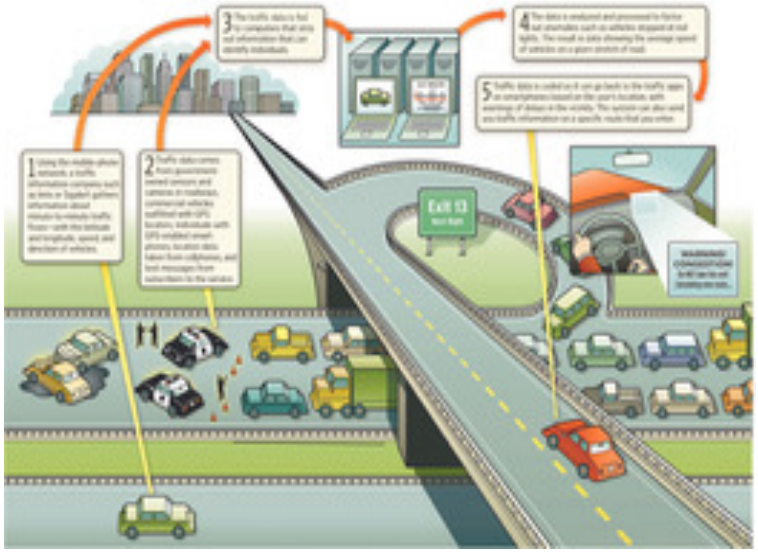
What can smartphone sensors do?

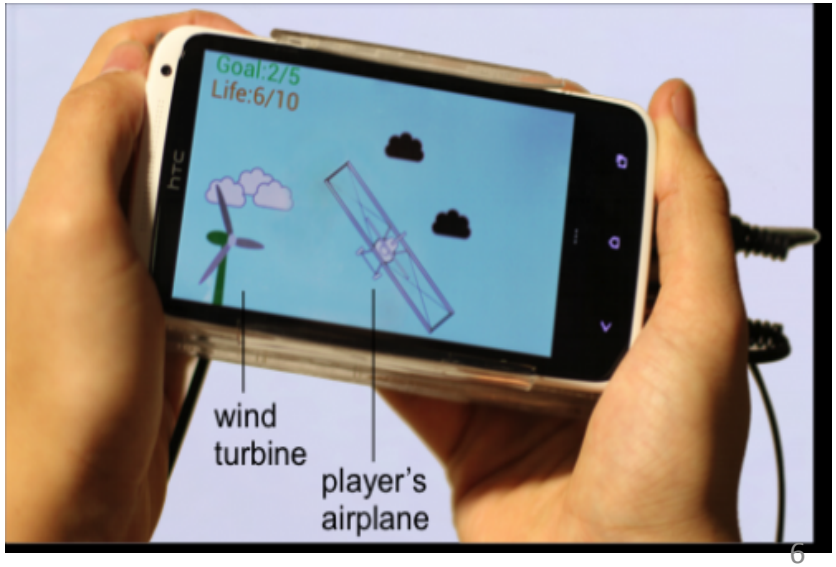
1. Side channels for sensing environment
2. Potential sources for device fingerprints.

- accelerometer
- gyroscope
- magnetometer
- ~~front and rear cameras~~
- NFC
- barometer
- speaker
- ~~microphone~~
- proximity
- light sensor
- Bluetooth
- ~~GPS~~
- ~~WiFi + cellular~~
- humidity
- temperature

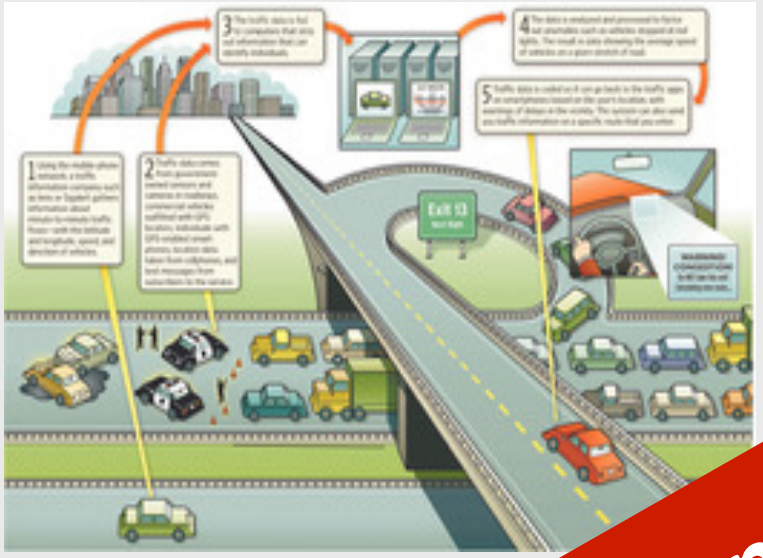
Can sensors be accessed freely?

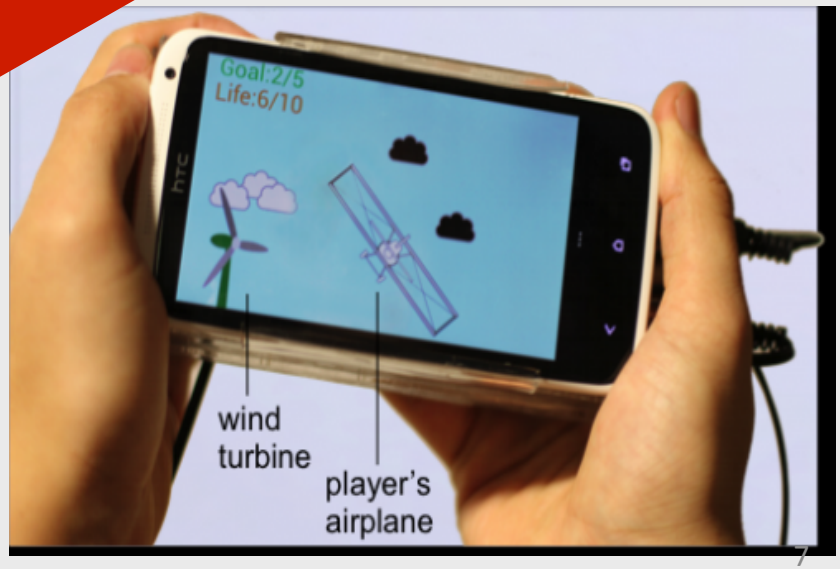
Most apps use motion sensors





Most apps use accelerometer





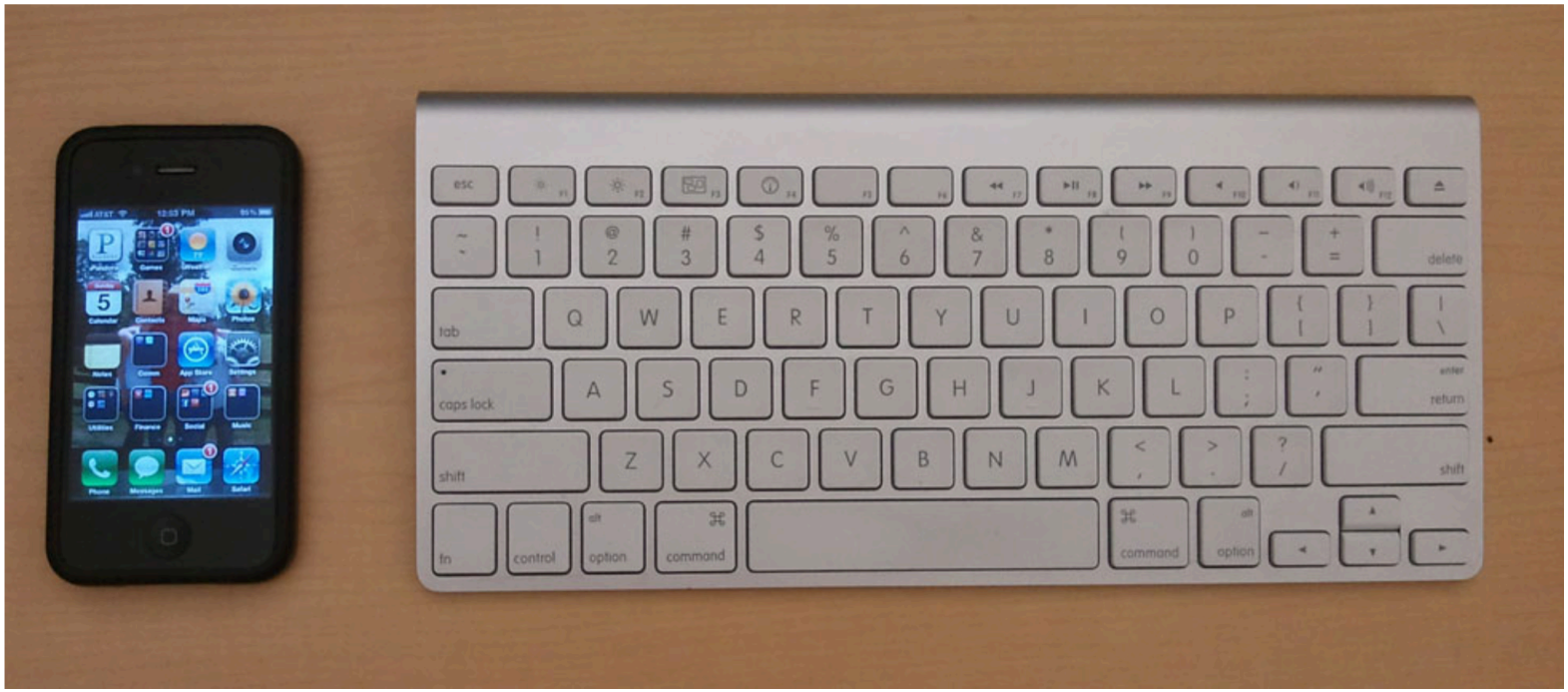
Is it safe to send motion data?

Sensors: Side Channels

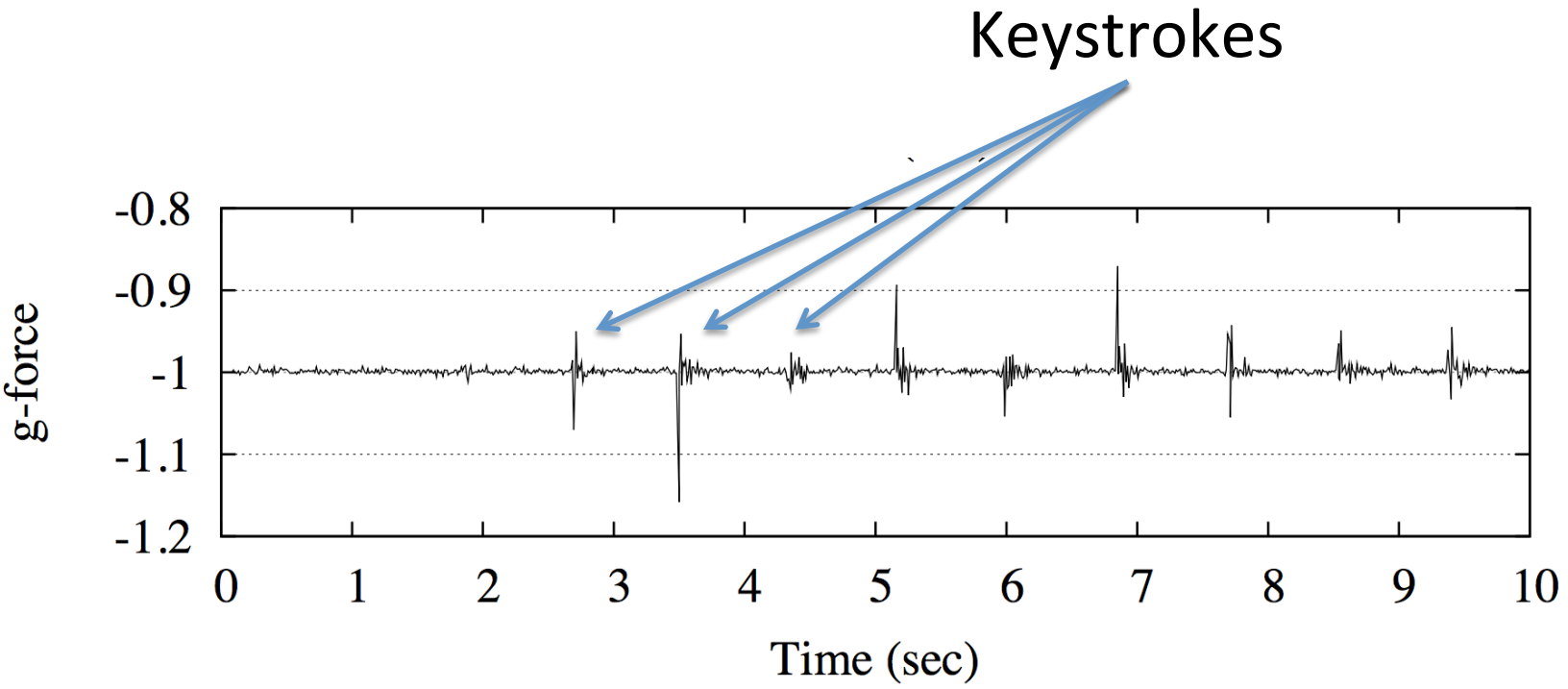
1. Accelerometers
2. Gyroscopes

(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers

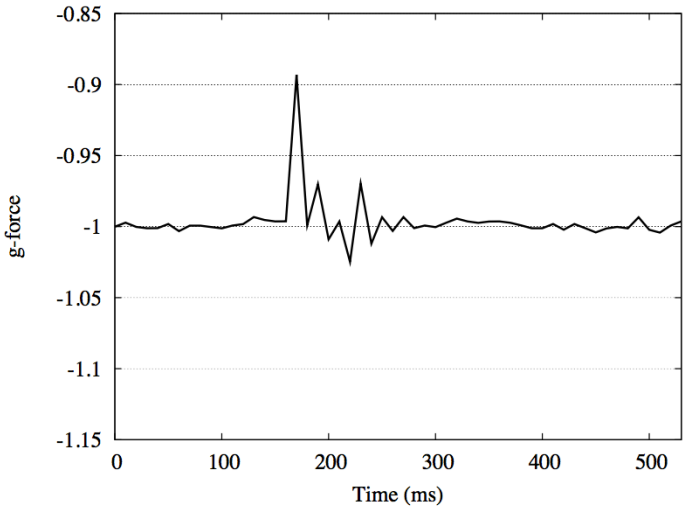
Decoding Keyboards Keystrokes Using Mobile Phone Accelerometers



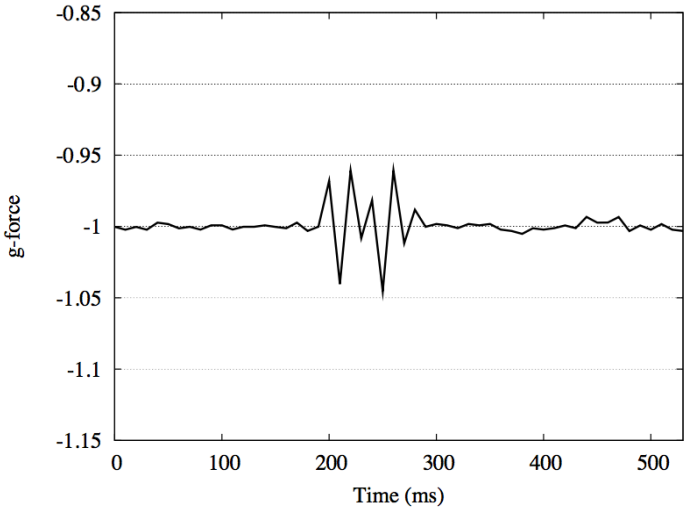
Keystrokes Sensed by Accelerometers



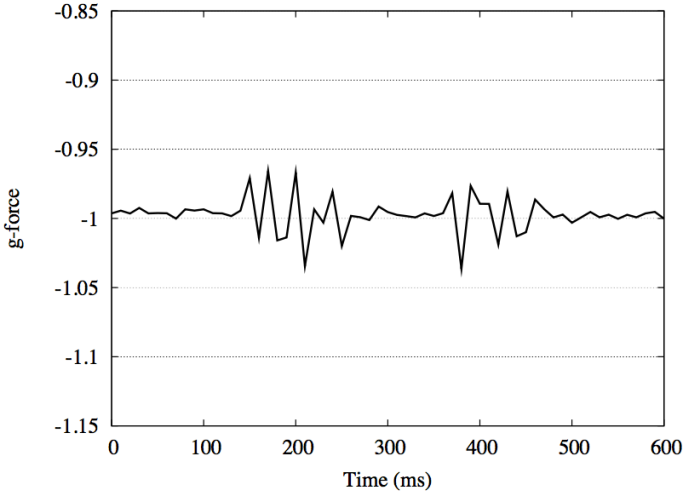
Keystrokes Sensed by Accelerometers



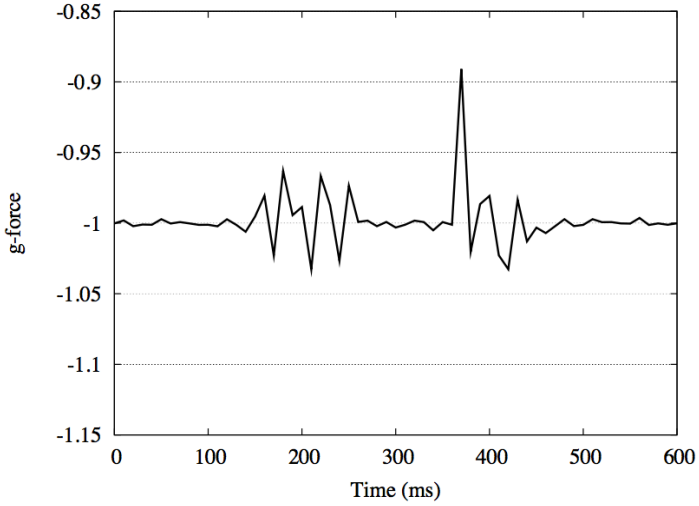
Single char “a”



Single char “l”



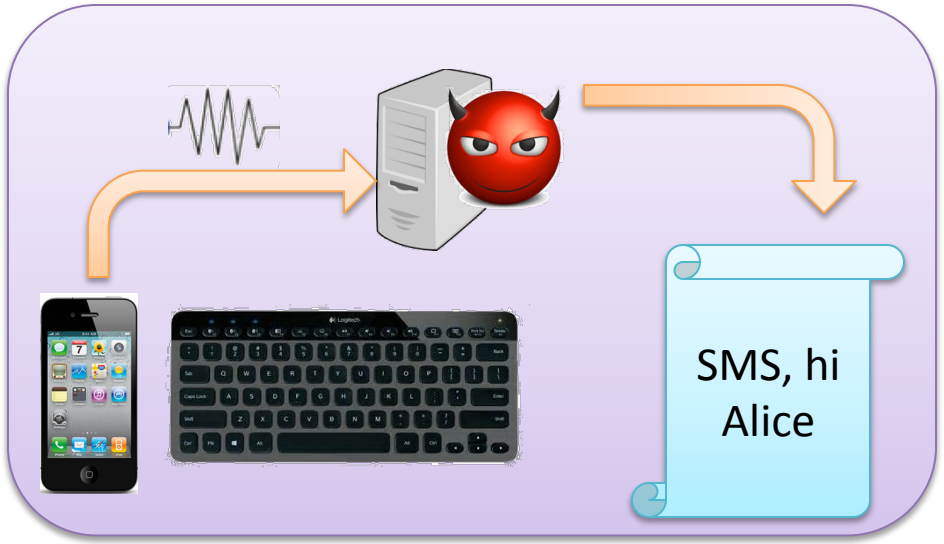
Character pair “nm”



Character pair “pq”

Attack scenarios

Install a malicious app



Record accelerometer data and recover keystrokes

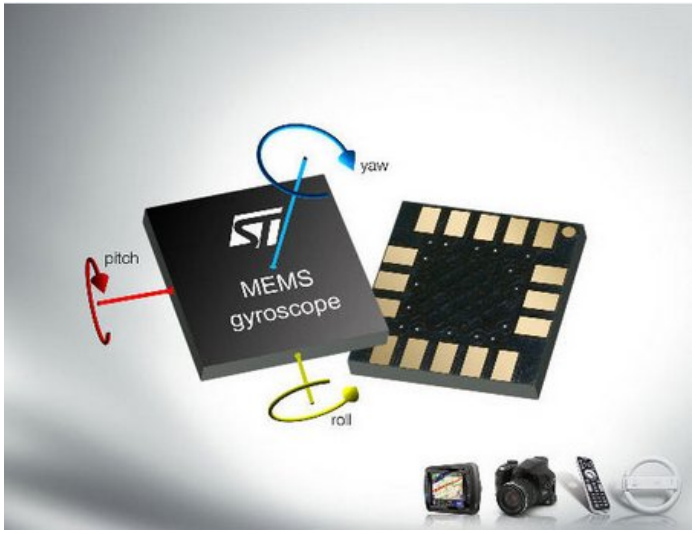
Results

1st or 2nd Choice Correct = 72.92%
L/R Accuracy =83.95%
N/F Accuracy = 64.88%

Typed Text: Glue the sheet to the dark blue background
Recovered Text: Glue *** sheet ** *** well hogs background blue

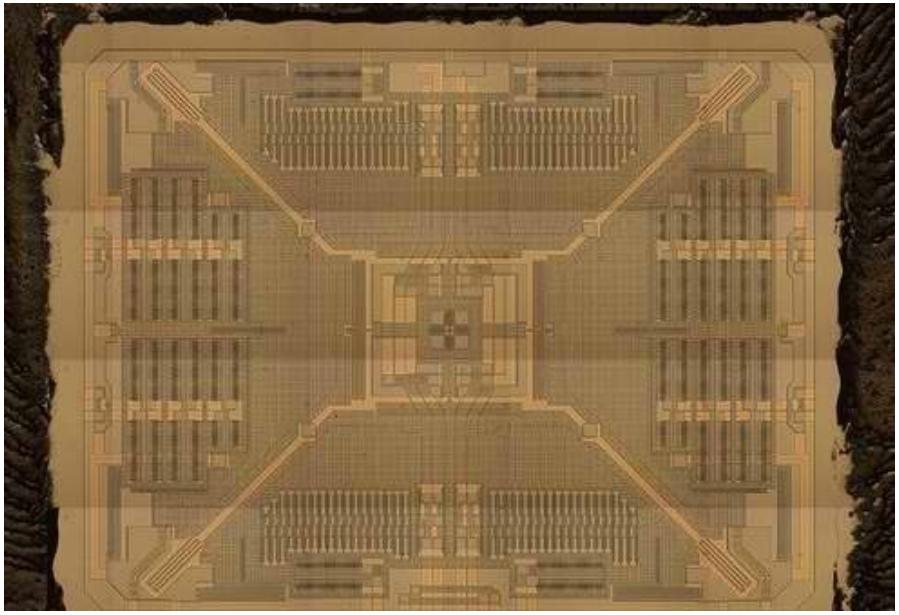
Typed Text: These days a chicken leg is a rare dish
Recovered Text: These days * chicken *** ** * rare dish

Gyrophone: Recognizing Speech From Gyroscope Signals

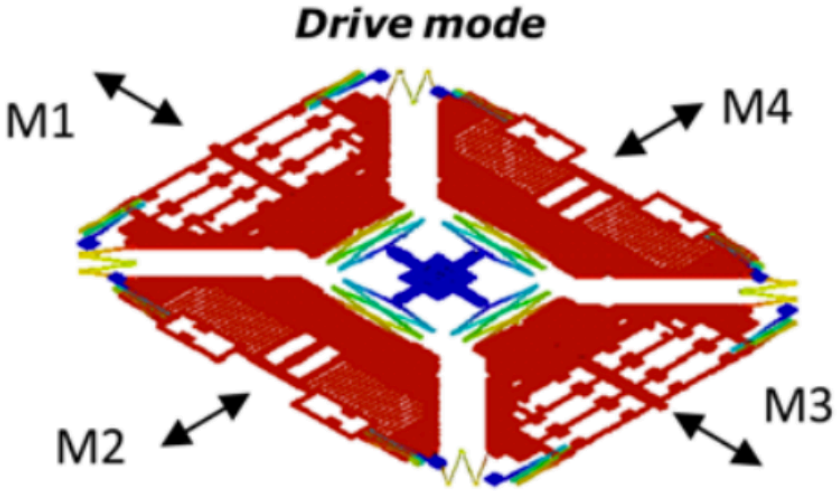


Gyroscope in Smartphones

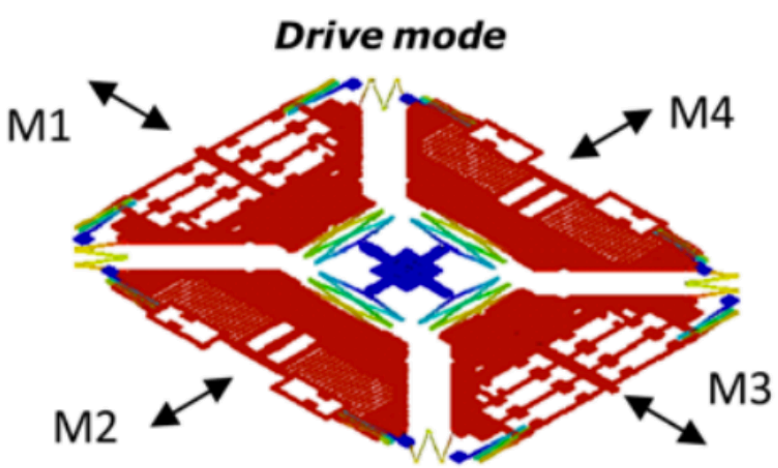
- Device used to measure or maintain orientation
- Works on the principals of angular momentum

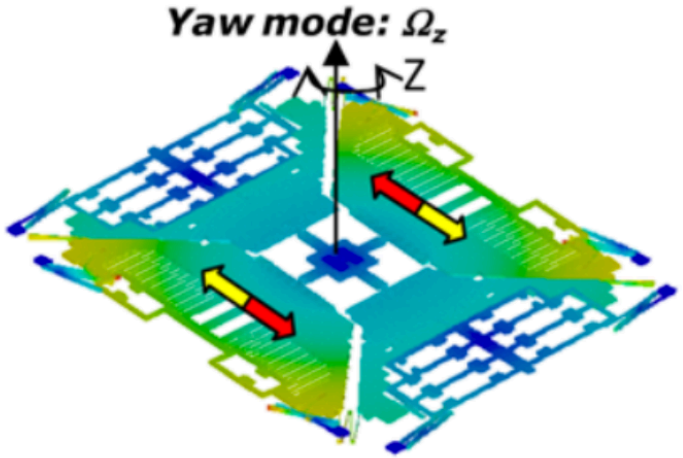


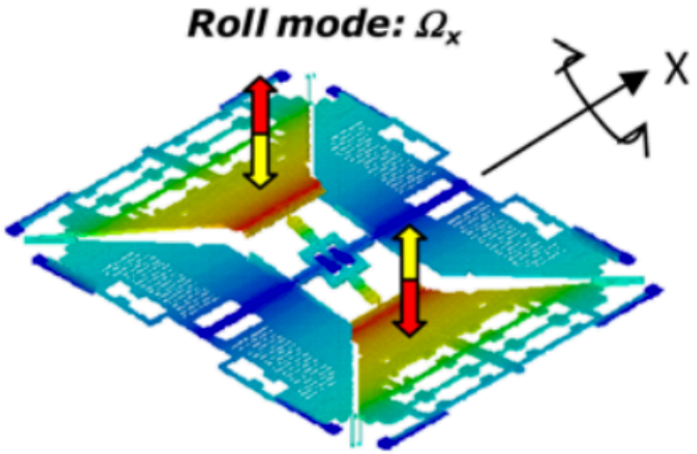
MEMS

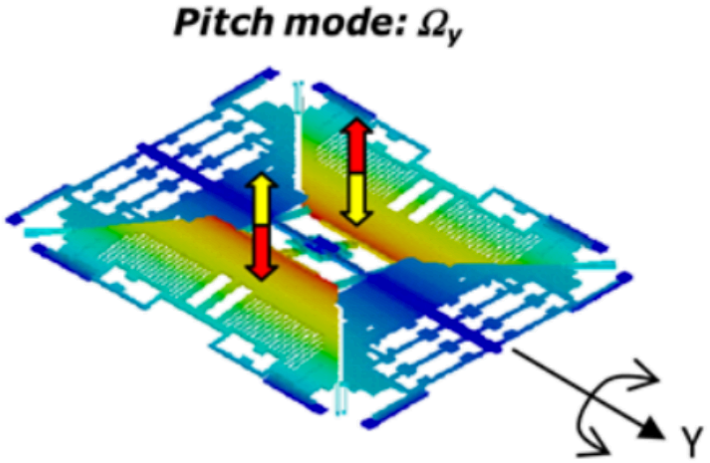


Gyroscope（MEMS）





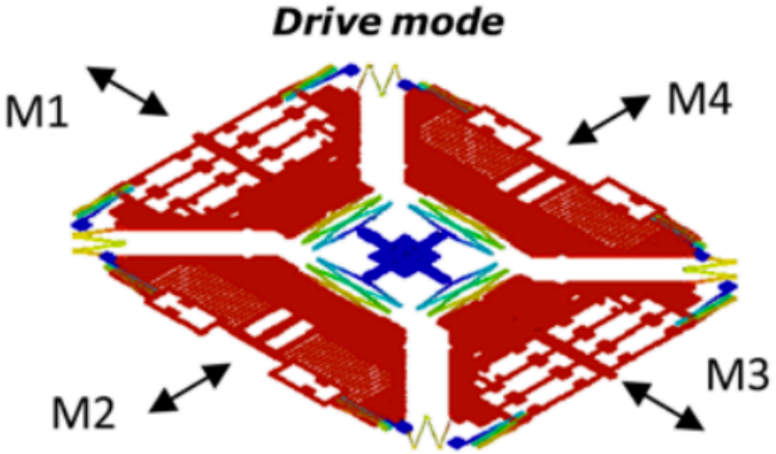




Acoustic Vibration

- Gyroscopes are sufficiently sensitive to measure acoustic vibrations.

- It is possible to recover speech from gyroscope readings; turn gyroscope into a crude microphone.



Results

- 50% success rate for speaker identification
- 65% success rate for number recognition

Device Fingerprints

Why Fingerprint Smartphones?

- Smartphones can be fingerprinted for:
  - Targeted Advertisement
  - Secondary Authentication factor

- Software based approaches:
  - Browser based features, Cookies
  - Different Firmware and Device drivers

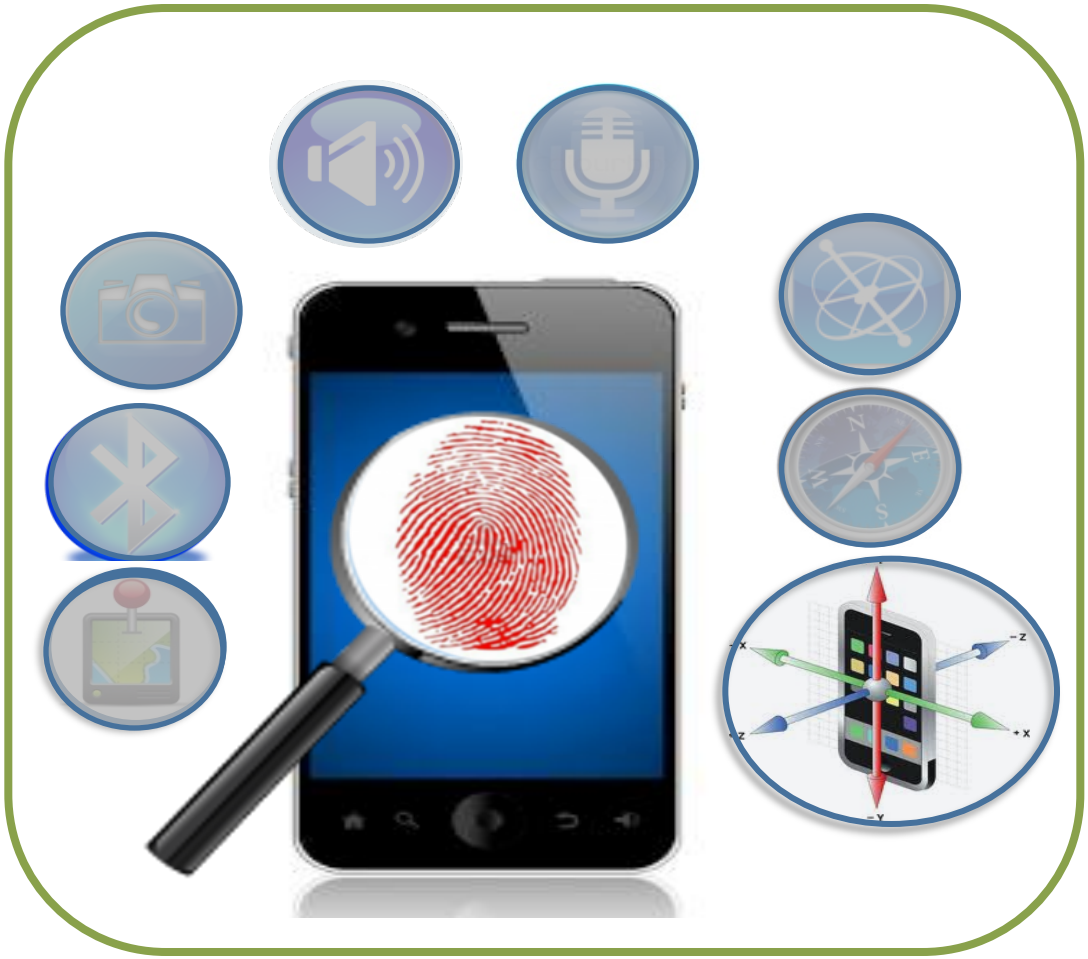
How can free app developers earn money?

- Advertisement
  - Advertisers provide prepackaged developer kits
  - Developers insert a few lines of code into their apps
  - Display ads→ side effect, collect data from devices
- Targeted advertisement
  - Track users

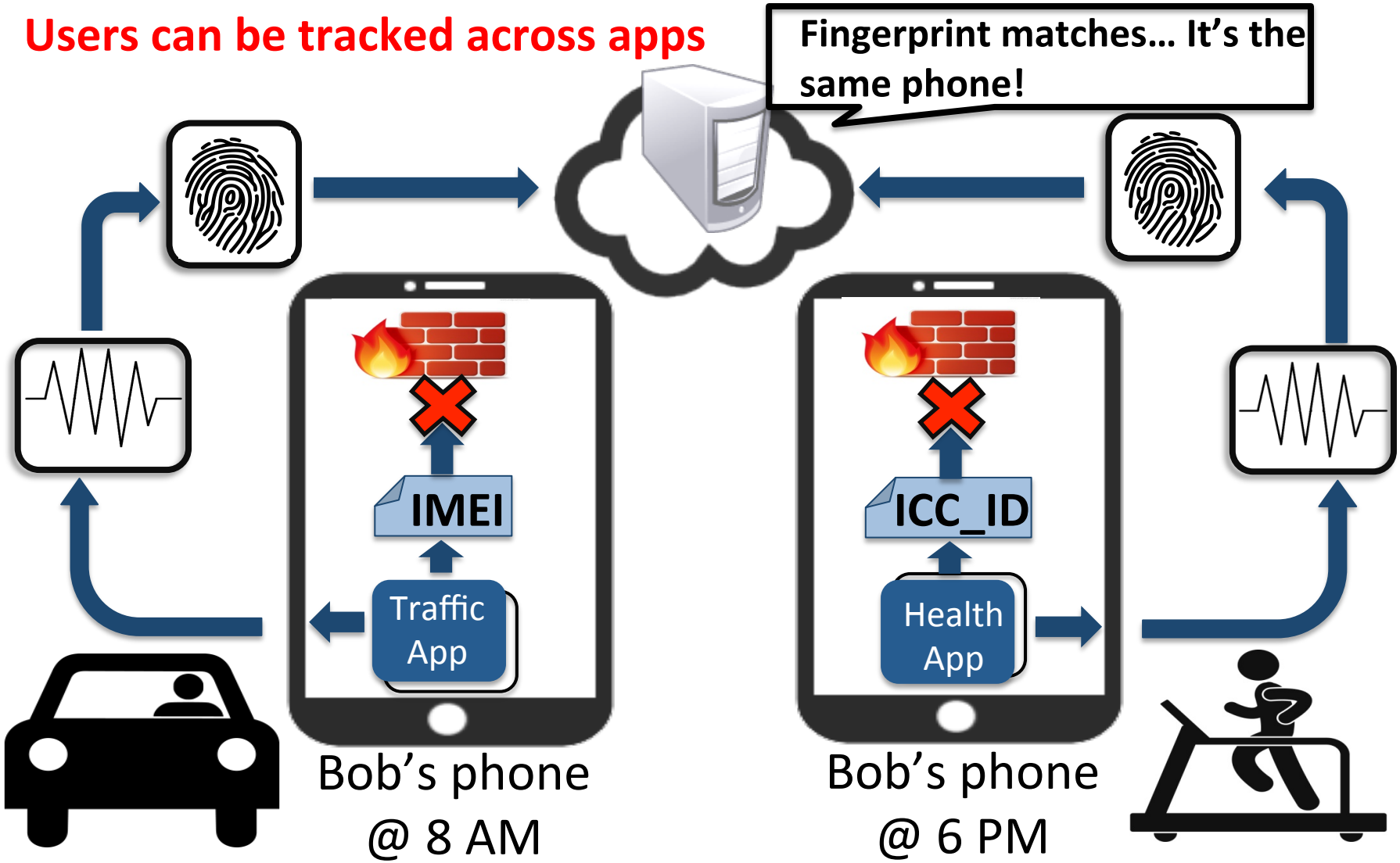
Some apps are sneaky

- Exchanging IDs without consent is rampant
  - IMEI (device id), IMSI (subscriber id), or ICC-ID (SIM card serial number) help track users
- Solution: TaintDroid
  - Realtime filtering of exchange of device IDs
- UDID for Apple devices has been removed since May 1, 2013 and IMEI for an Android Device requires explicit permission.

Our finding: Accelerometers have fingerprints



What if accelerometers have fingerprints?



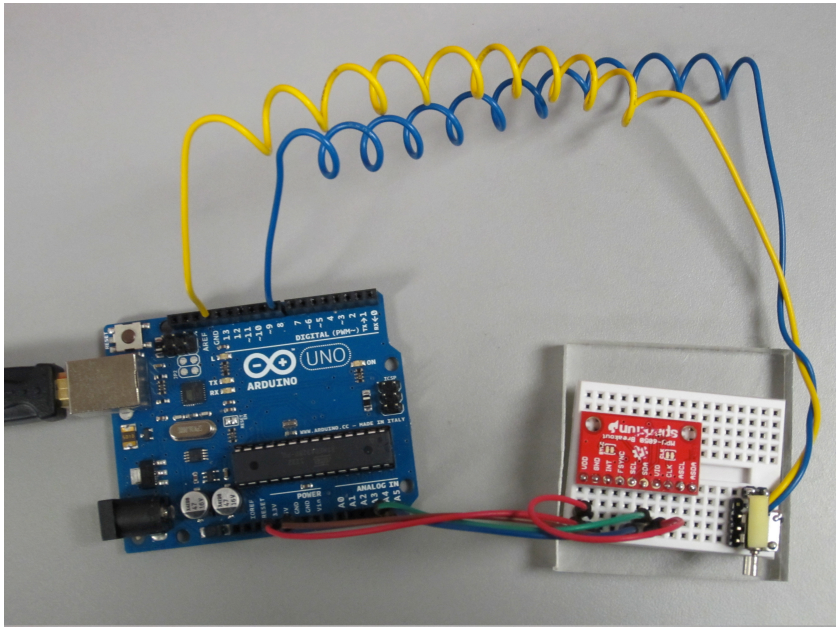
Why is this an important threat?

- Enables tracking of users across apps
  - Without an explicit cookie
- Fingerprint is intrinsic to the hardware
  - Software update won't erase it
- A slice of sensor data can identify device
  - New wearable devices send more sensor data

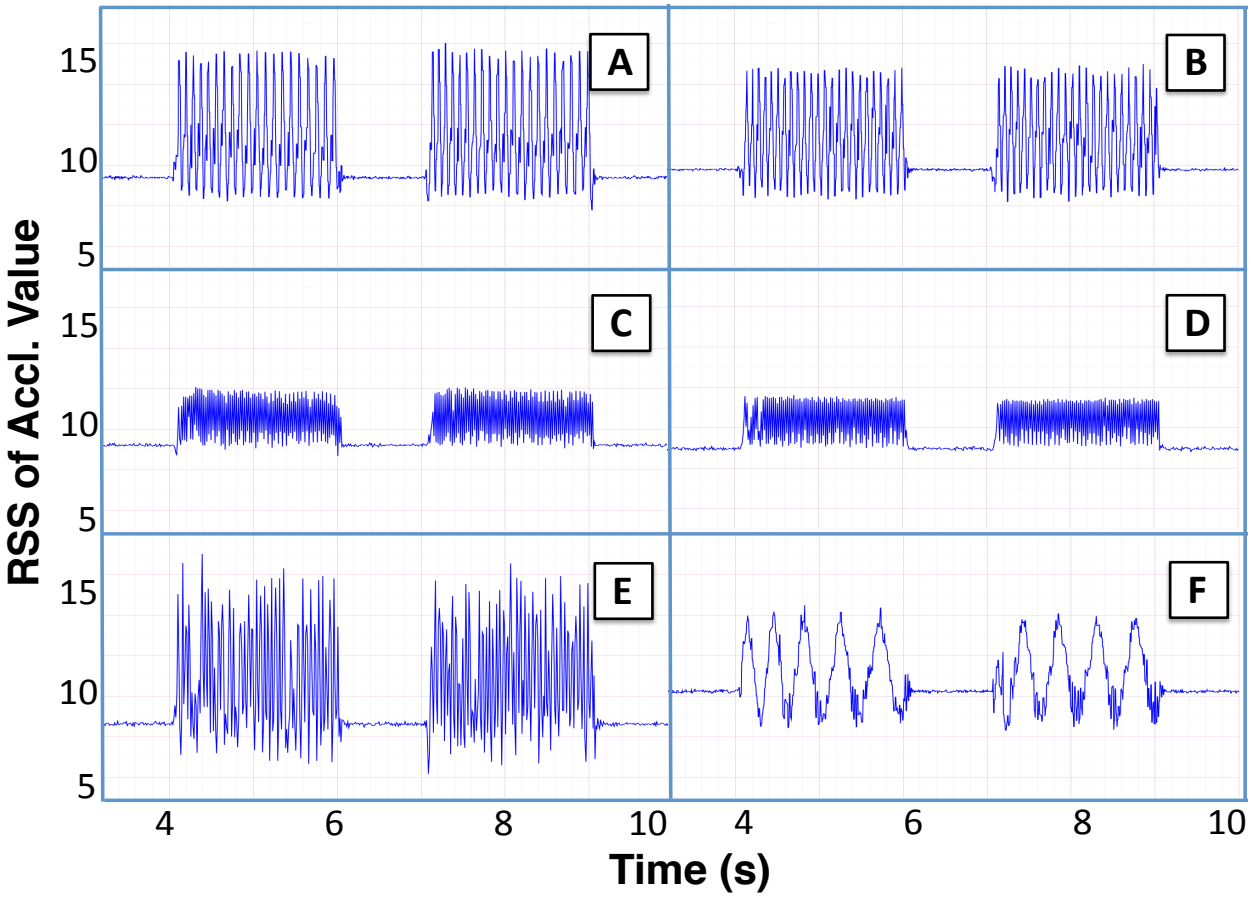
Accelerometers are distinct

Experimental setup

- Six stand-alone accelerometer chips (used in many mobile devices such as Galaxy S III and Kindle Fire)
- Stimulation with an external vibration motor (used in most smartphones)
- Arduino to control vibration and collect accelerometer readings

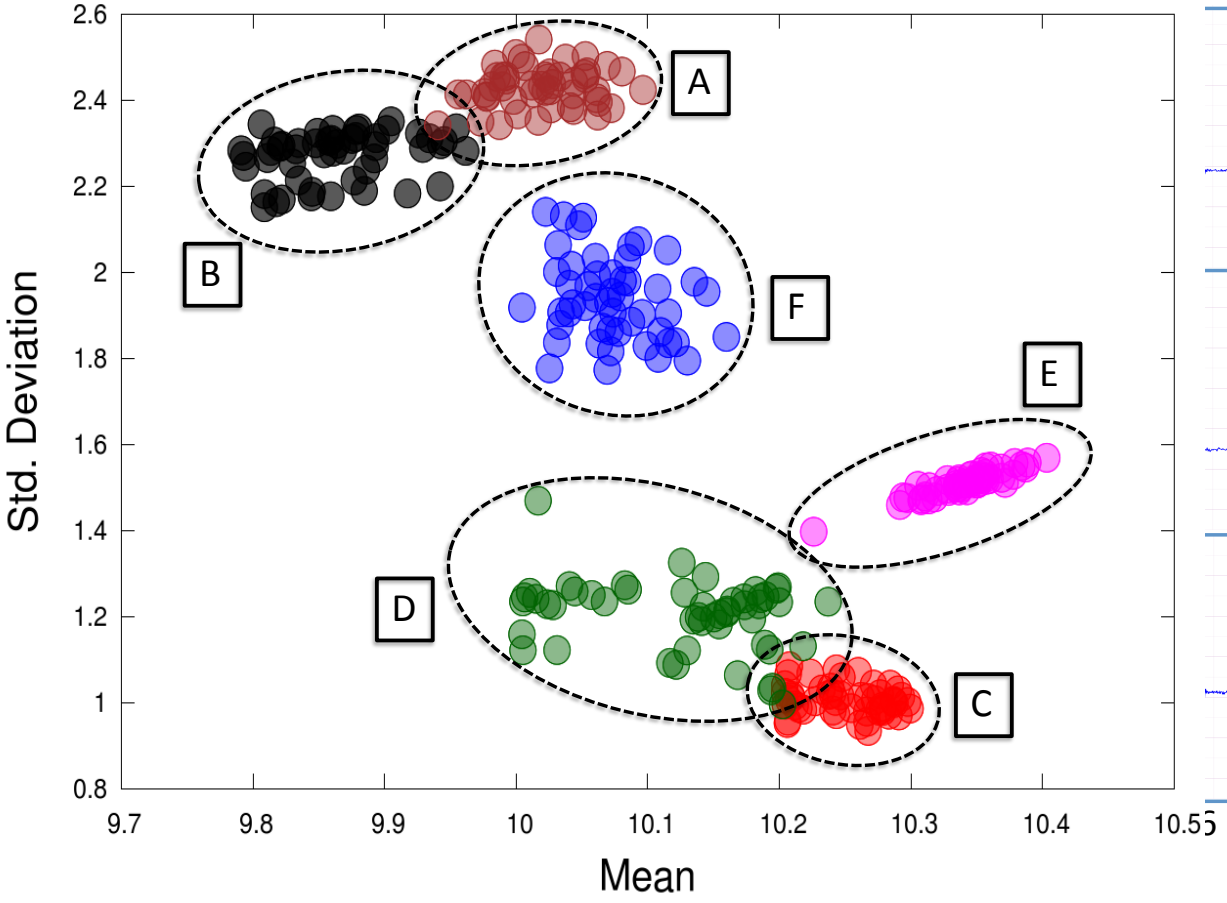


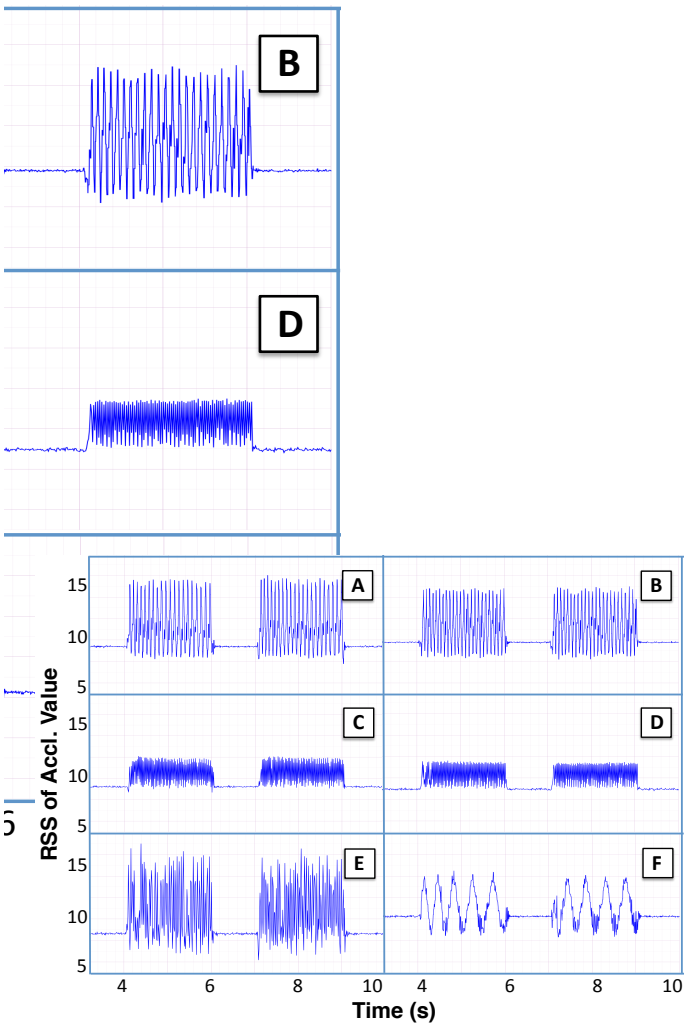
Accelerometers are distinguishable



Accelerometers yield distinct responses for the same vibration

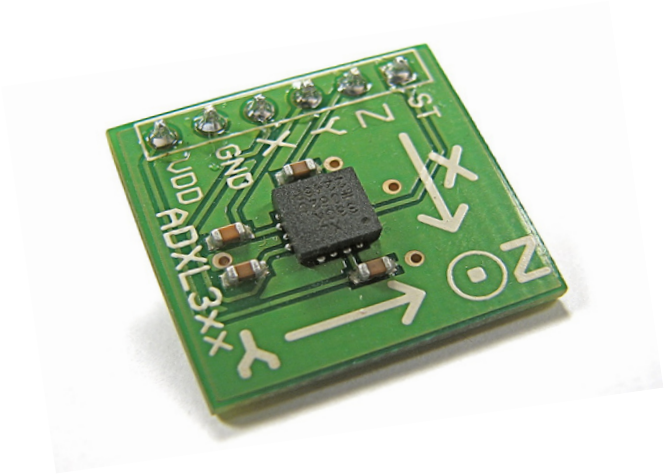
Accelerometers are distinguishable



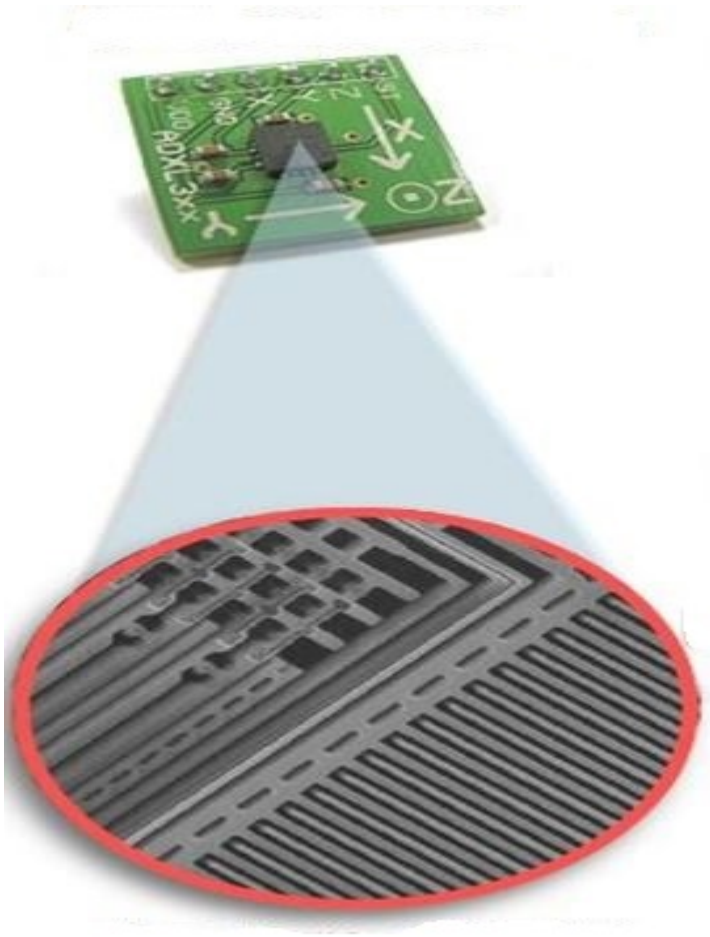


Why are accelerometers distinct?

Accelerometers are based on MEMS

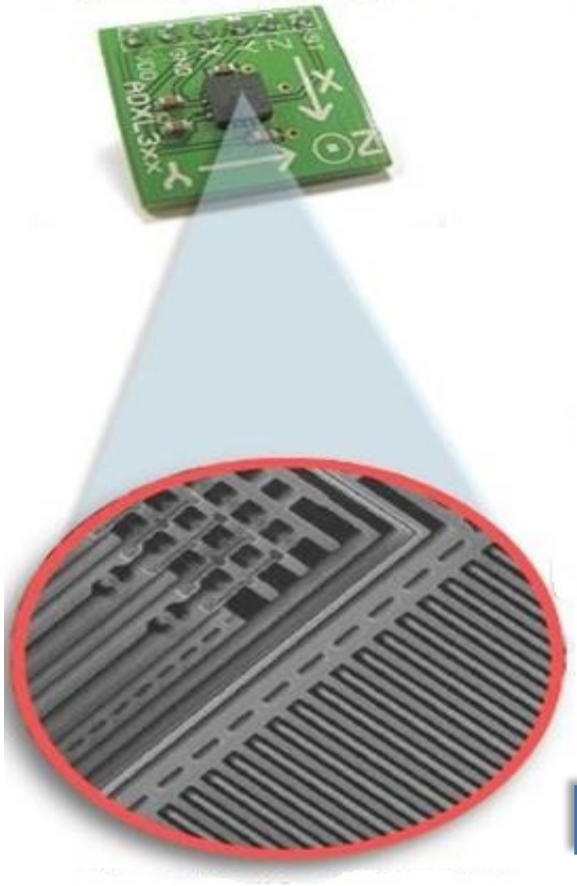


Internal structure of an accelerometer

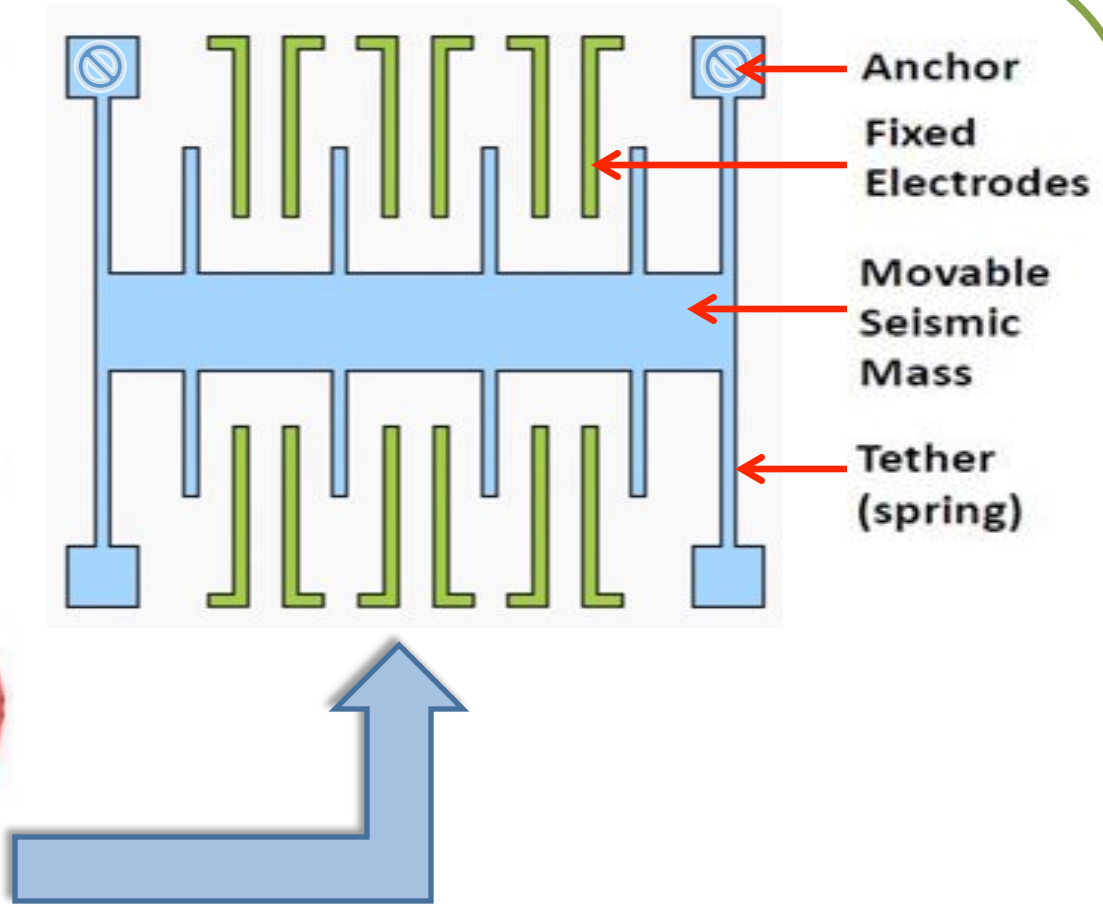


Internal structure of an accelerometer

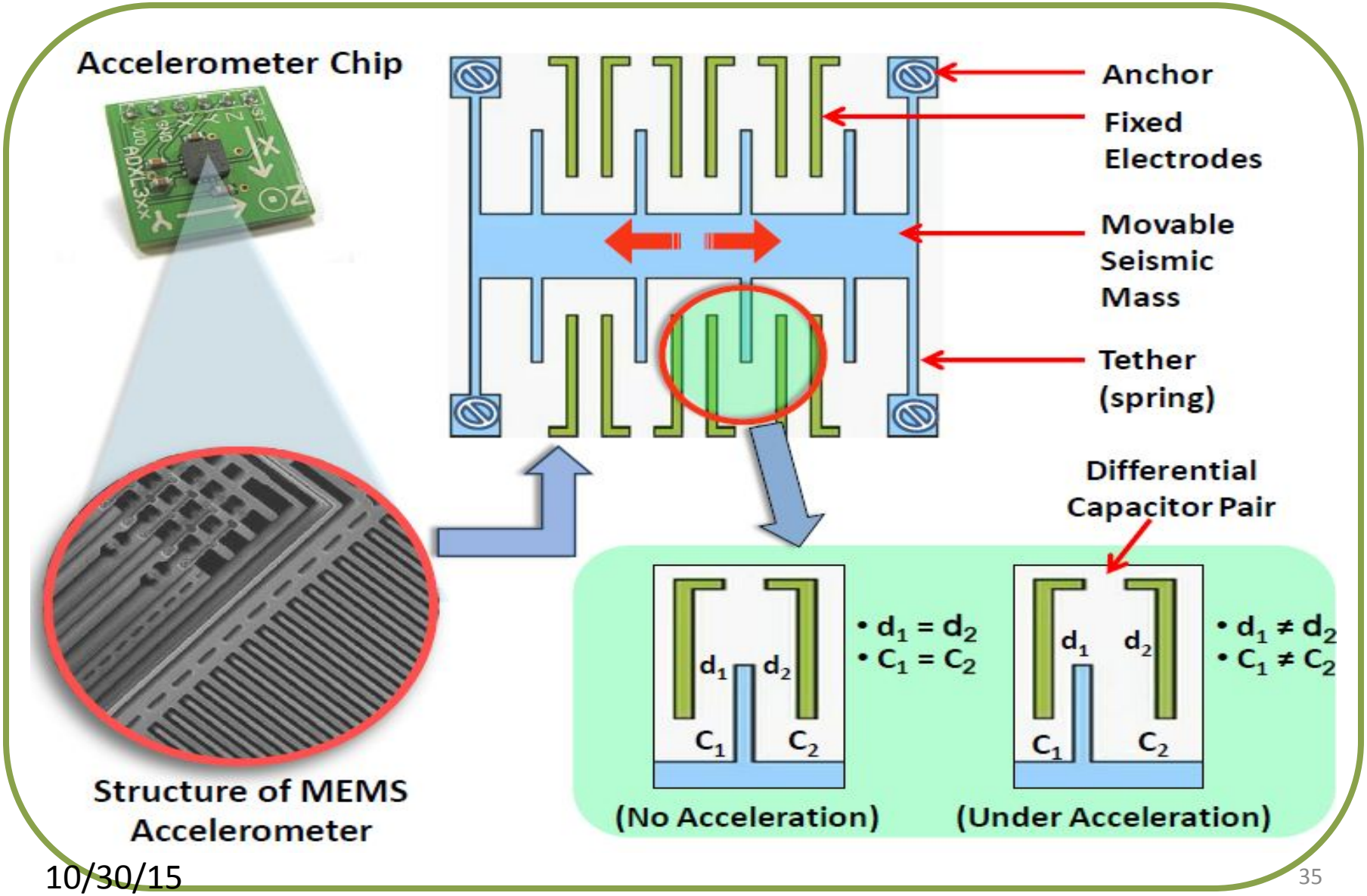
Accelerometer Chip



Structure of MEMS accelerometer

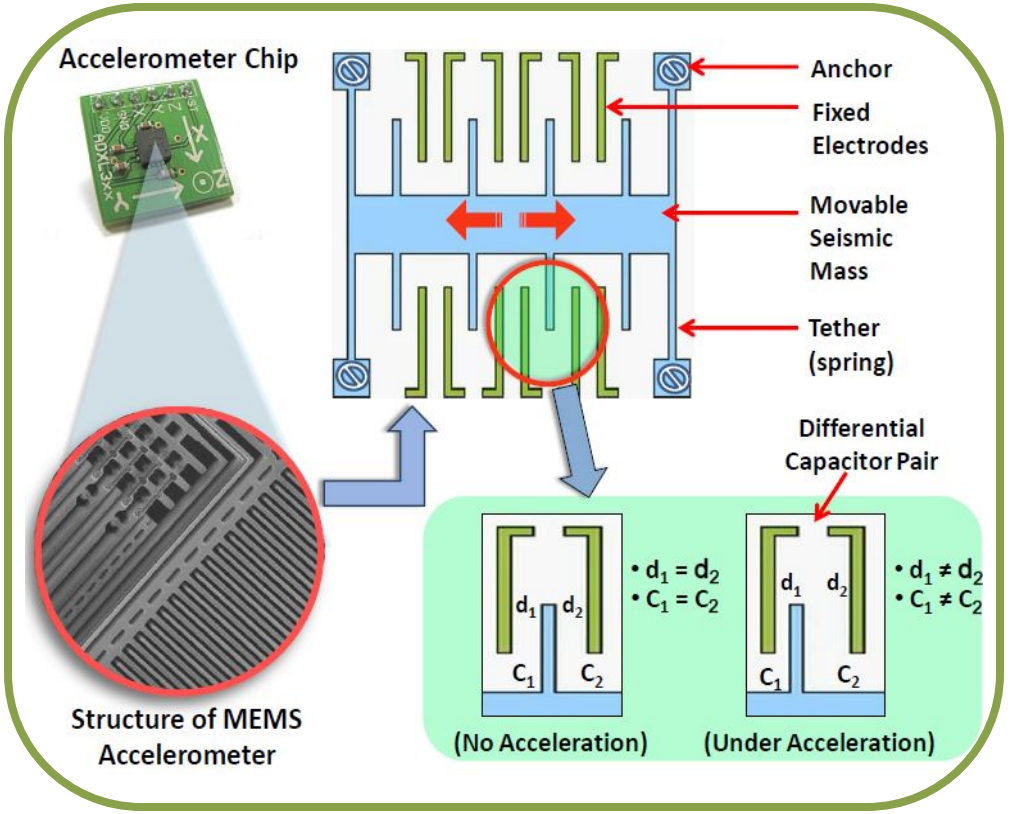


Internal structure of an accelerometer



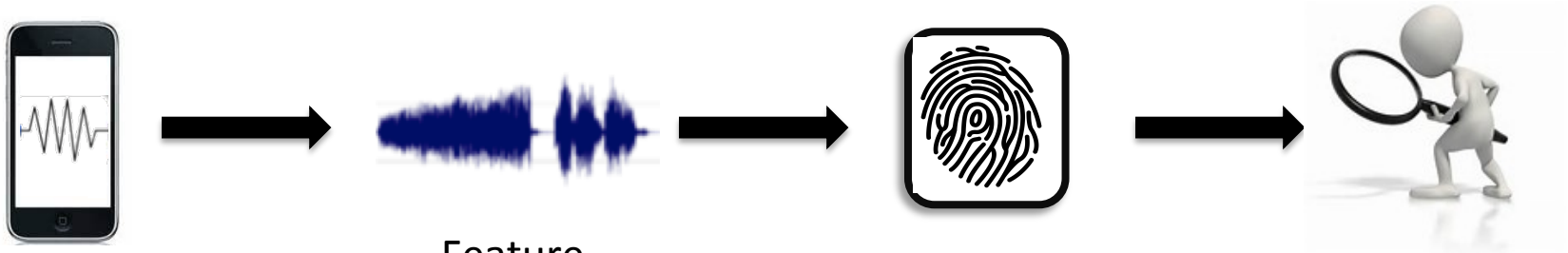
Reasons for difference in accelerometers

- Manufacturing imperfections
  - Slight gaps between structural parts can change the capacitance
- Subtle imperfections do not alter the rated functionality
  - Apps (display rotation, fitness monitoring, motion based games) work as expected
- Produced at low cost
  - No need to be more precise than app requirements



How to extract the fingerprint?

Fingerprinting Accelerometers



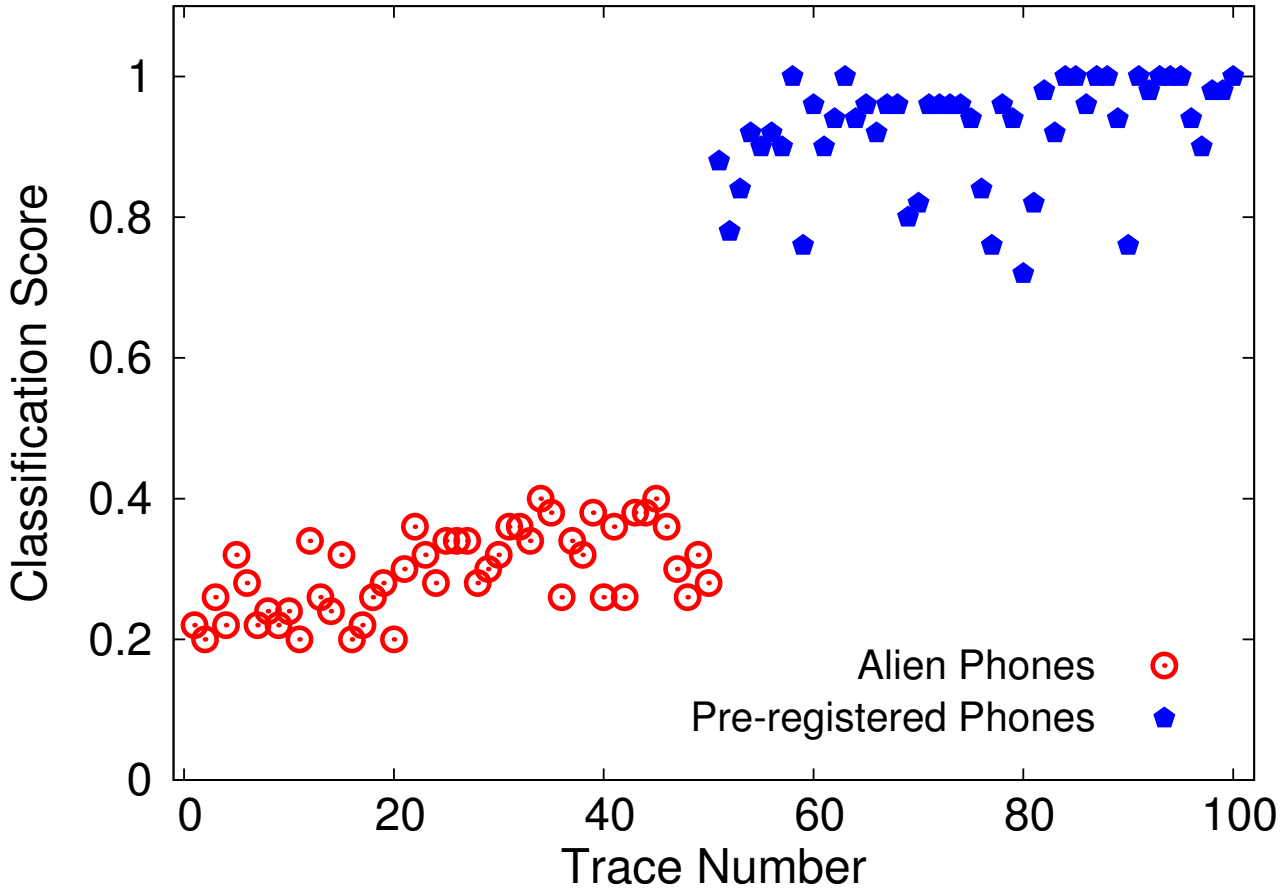
Smartphone
Data collection

Feature
Extraction

Fingerprint
Creation

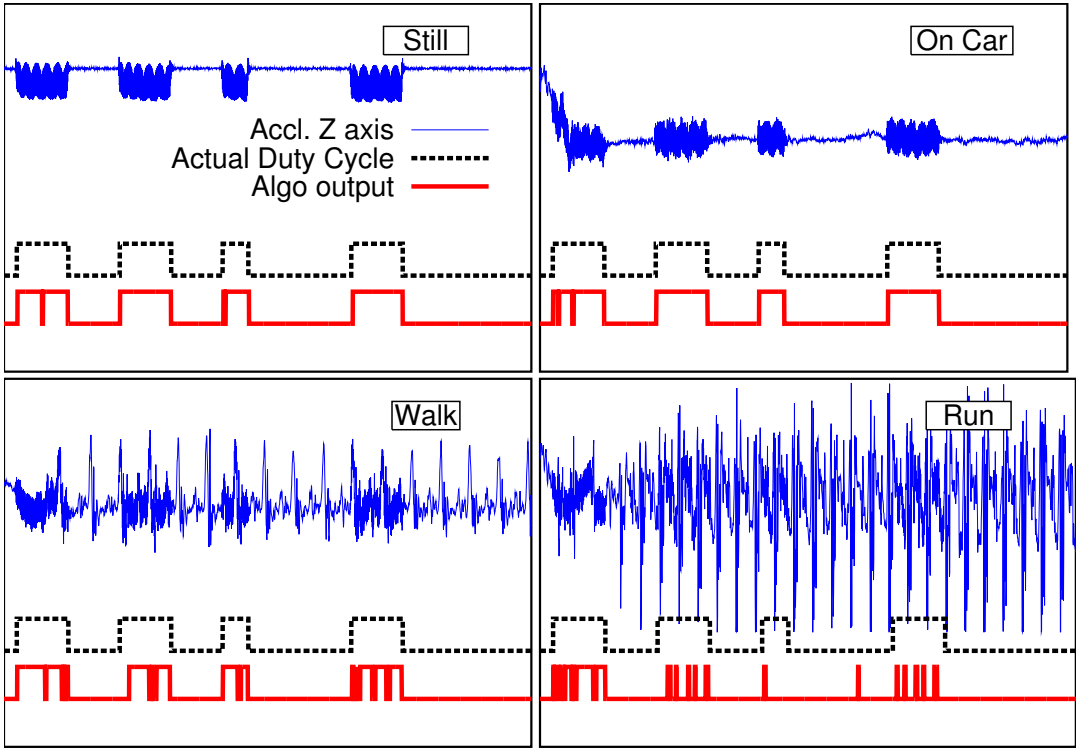
Fingerprint
Matching

Can we distinguish between an alien phone from a registered phone?



When to extract a fingerprint in practice?

- Opportunistically under similar conditions
  - e.g. when vibration motor on, CPU load moderate



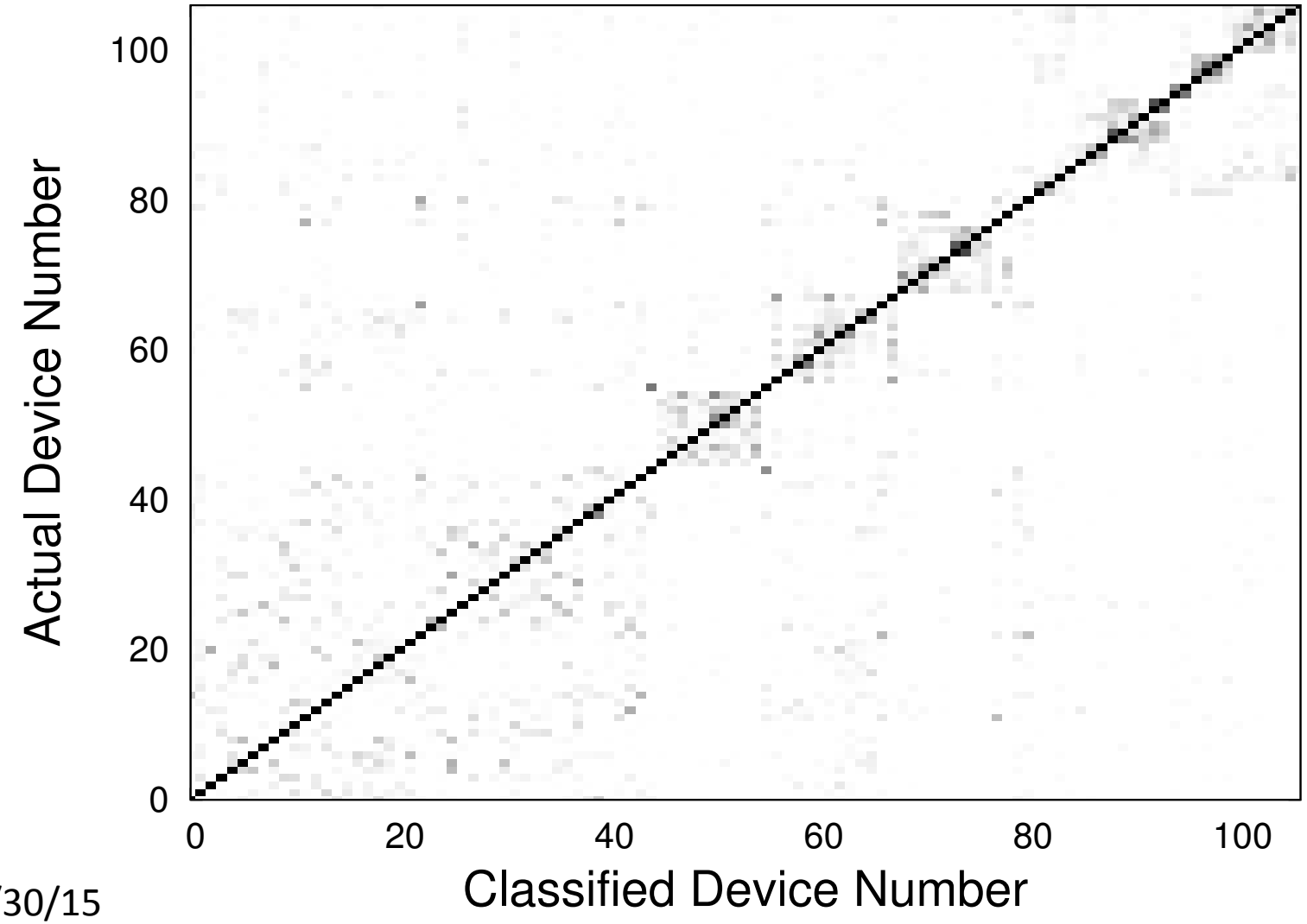
How robust are the fingerprints?

Evaluation Setup

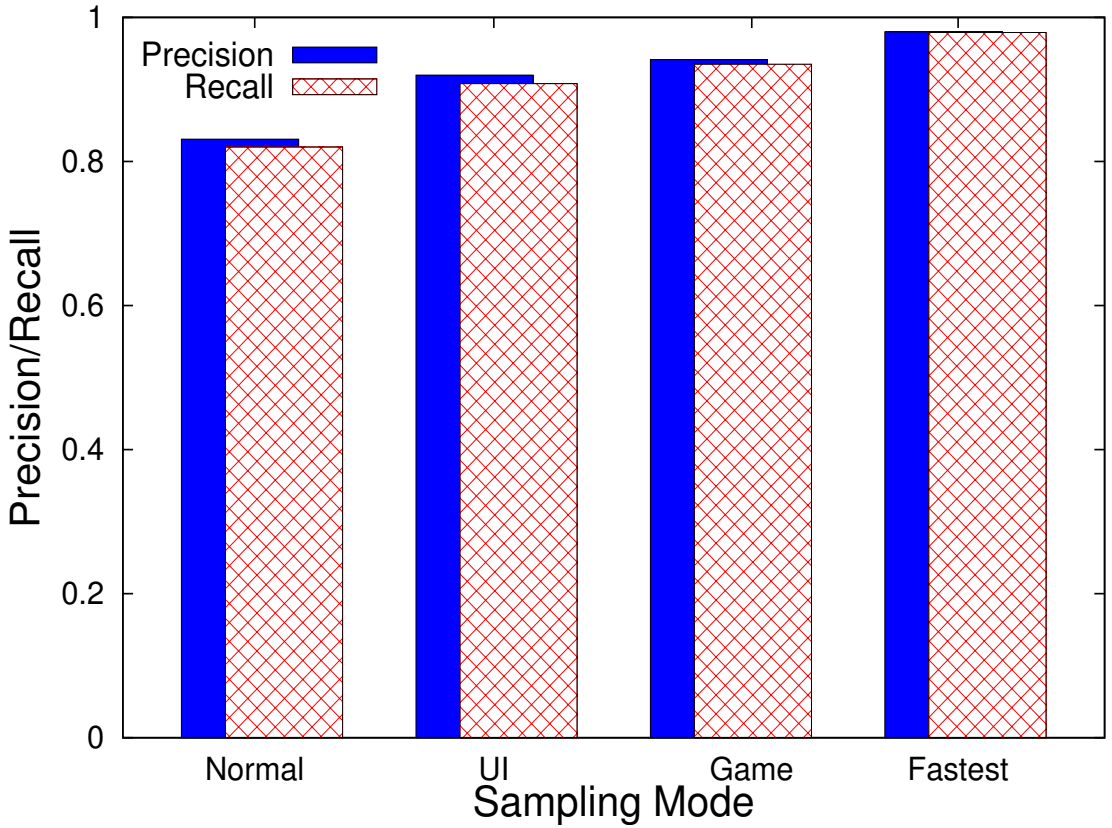
- Devices
  - 80 stand-alone accelerometer chips
  - 27 Android smartphones/tablets of 6 models
- Metrics
  - Average Precision: $\frac{1}{k}\sum_{i=1}^{k}\frac{TP_i}{TP_i + FP_i}$
  - Average Recall: $\frac{1}{k}\sum_{i=1}^{k}\frac{TP_i}{TP_i + FN_i}$
  - Accuracy: $\frac{1}{n}(\sum_{i=1}^{k} TP_i + \sum_{j=1}^{l} TN_j)$

k trained classes, l alien classes, and n test traces

Overall likelihood of misclassification



Does the fingerprint manifest only at faster sampling rates?



- Even at slower sampling rates, devices exhibit discriminating features
- Likelihood of distinguishing devices improves with faster sampling rates

Sensors offering side channel not new

- Sniffing for side channel attack for inferring key-strokes like TouchLogger, ACCessory, Taplogger etc.
  - Keyboard acoustic analysis
  - Time Events
  - Software specialization
- Fix: disable accelerometer during sensitive operation
- A small slice of sensor data adequate for fingerprinting

Summary

- Sensors can create side channel to leak sensitive information
  - Accelerometers to sense keystrokes
  - Gyroscope as a coarse microphone

- Due to the imperfection of sensors, sensors have their fingerprints
  - Accelerometers possess fingerprints
  - Can act like a cookie in tracking users