RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: MBS-F01

Side-Channels in the 21st Century: Information Leakage From Smartphones

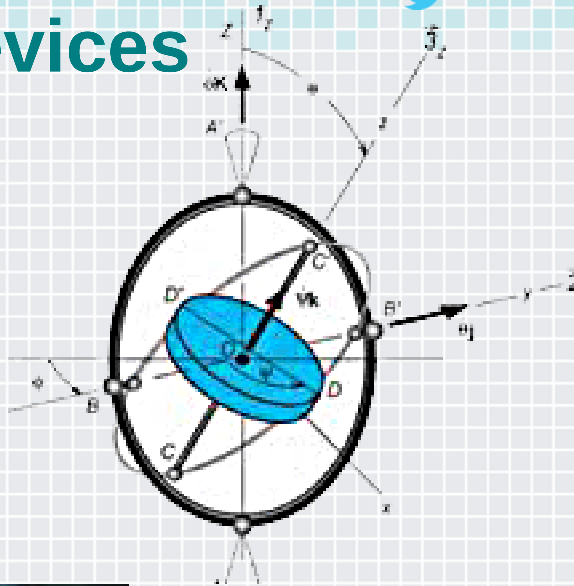
Gabi Nakibly, Ph.D.

National Research & Simulation Center
Rafael – Advanced Defense Systems Inc.
gabin@rafael.co.il

Yan Michalevsky

Stanford University
yanm2@cs.stanford.edu

Side-Channel Attacks on Mobile Devices

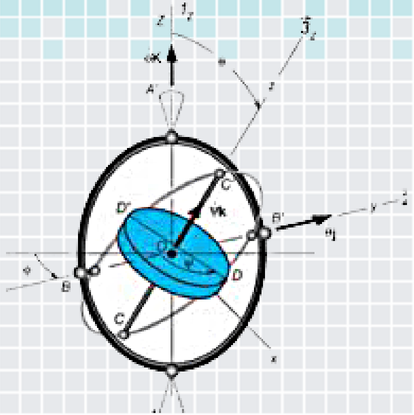


Session's Main Points

- Mobile devices are susceptible to information leakage in weird and unexpected ways.
- Rogue applications might do harm even if they have few permissions.
- The bottom line: treat every app you install as having 'root' on the phone.
  - After this presentation you will think twice before installing a "harmless" game from an unofficial market having "zero" permissions.

RSA Conference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Sensor ID: Mobile Device Identification via Sensor Fingerprinting

H. Bojinov, Y. Michalevsky, G. Nakibly and D. Boneh

Mobile device identification

- The research question: Can an app (or a website) identify the device on which it runs?
- Answer: Yes!
  - Android: Device ID, Serial number, MAC Address, ANDROID ID.
  - iOS :UDID, identifierForVendor, advertisingIdentifier, MAC Address.

Mobile device identification (cont.)

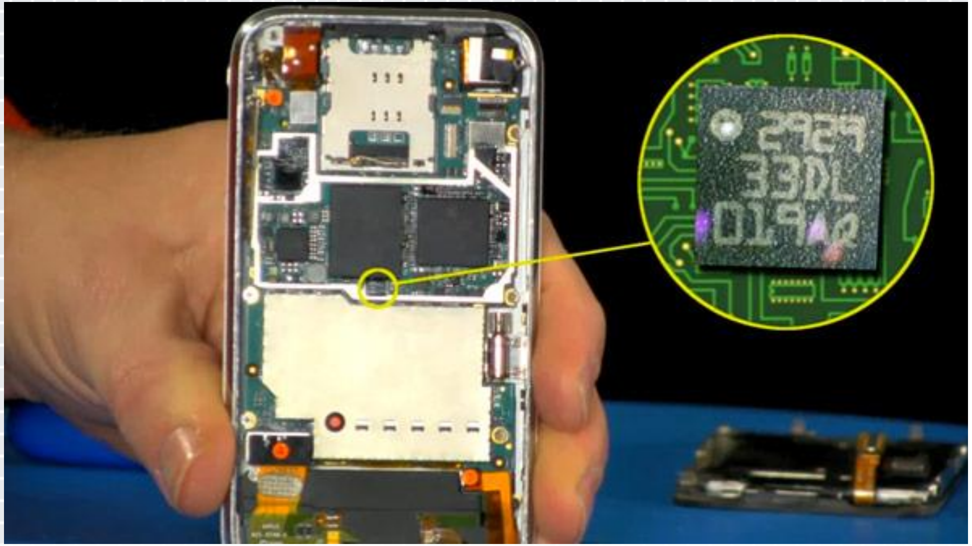
- However, all of these standard identifiers either
  - require the user's permission
  - can be changed by the user
  - does not survive factory reset
  - not good for all mobile device types
  - can not be used by a web application

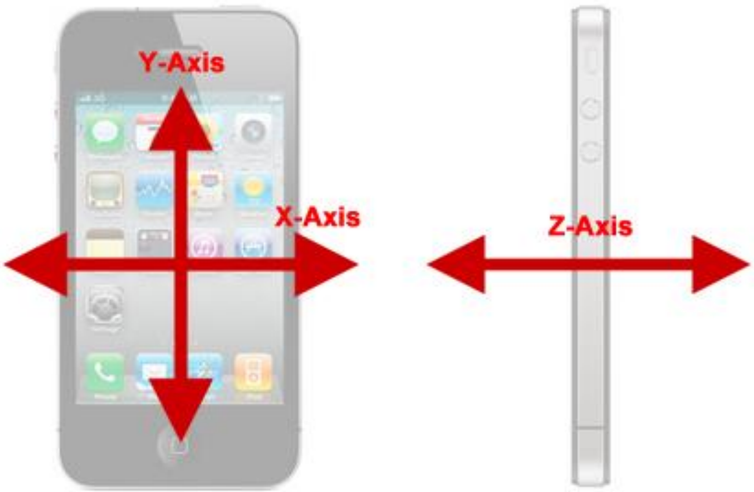
The Basic Idea

- Each sensor has a tiny inaccuracy that is very specific to it.
- Such inaccuracies can be used to fingerprint the device.

Accelerometer

- Measures the acceleration of the phone in all three directions.





Accelerometer Skew

$$a_m = a_t \cdot S + O$$

measured acceleration

actual acceleration

sensitivity (ideally = 1)

offset (ideally = 0)

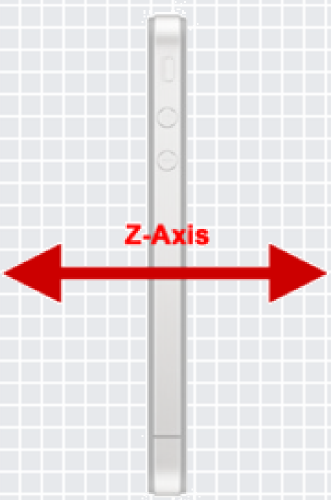
But how can we measure S and O?

- We need some reference acceleration…


GRAVITY

Measuring S and O

- As a first step we tried to identify S and O for the Z axis

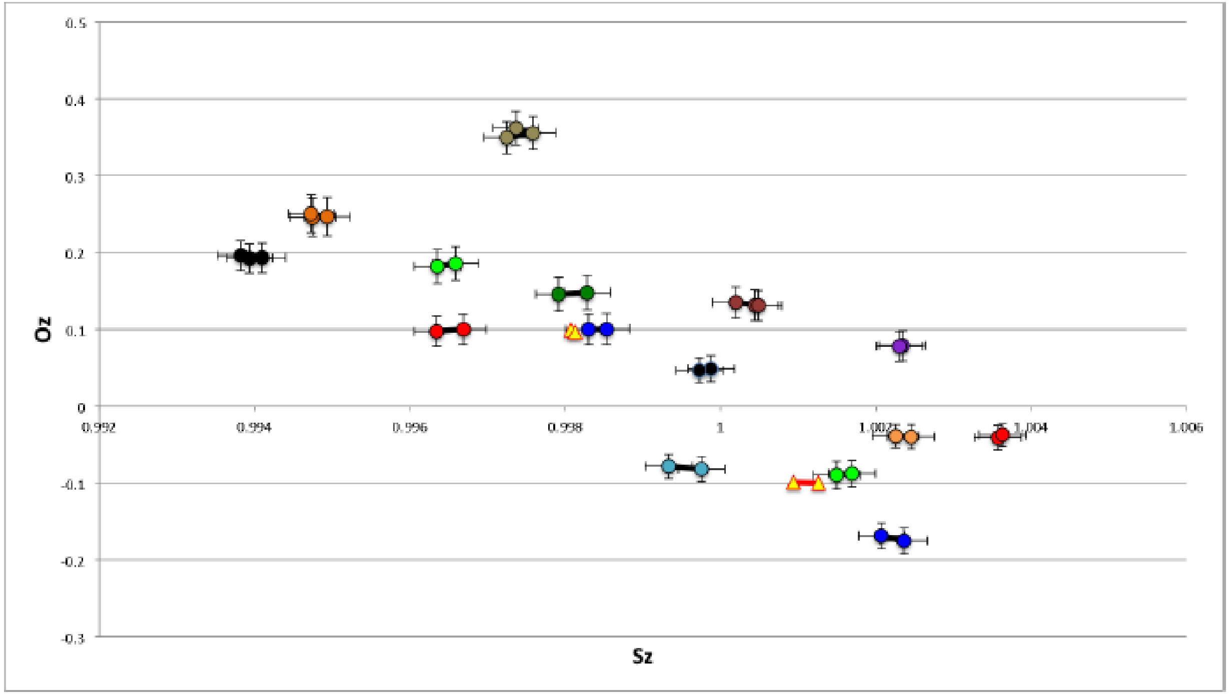


Measuring S and O

- Measure the acceleration face up and then face down and then do some calculations

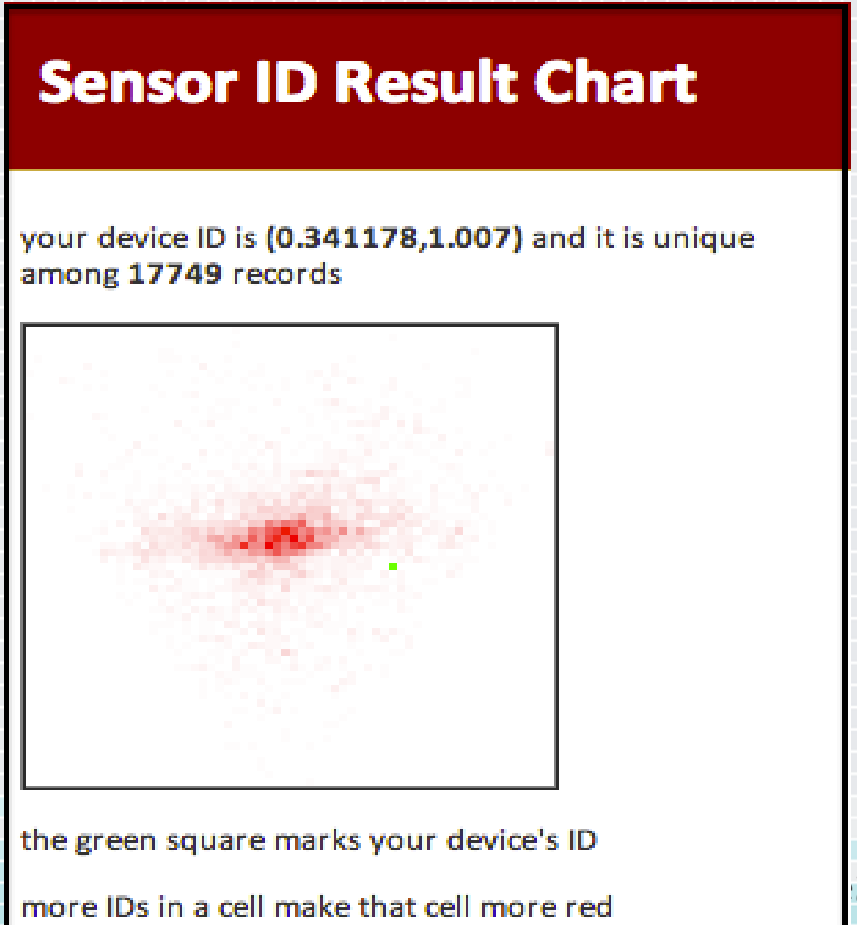
$$S_z = (z_{m^+} - z_{m^-})/2g$$
$$O_z = (z_{m^+} + z_{m^-})/2$$

Initial Experiment for 17 iPhones



Results for 10,000(!) phones

- An estimated **7.5 bits** of identification.
- If we can measure S and O for all three axes we can get 3*7.5 = **22.5 bits** of identification.



RAFAEL ADVANCED DEFENSE SYSTEMS LTD.

Measuring S and O for all axes

- A phone does not usually stand up…
- Alternatively, we can measure the phone is 6 resting positions.

Measuring S and O for all axes

- And then do some math….

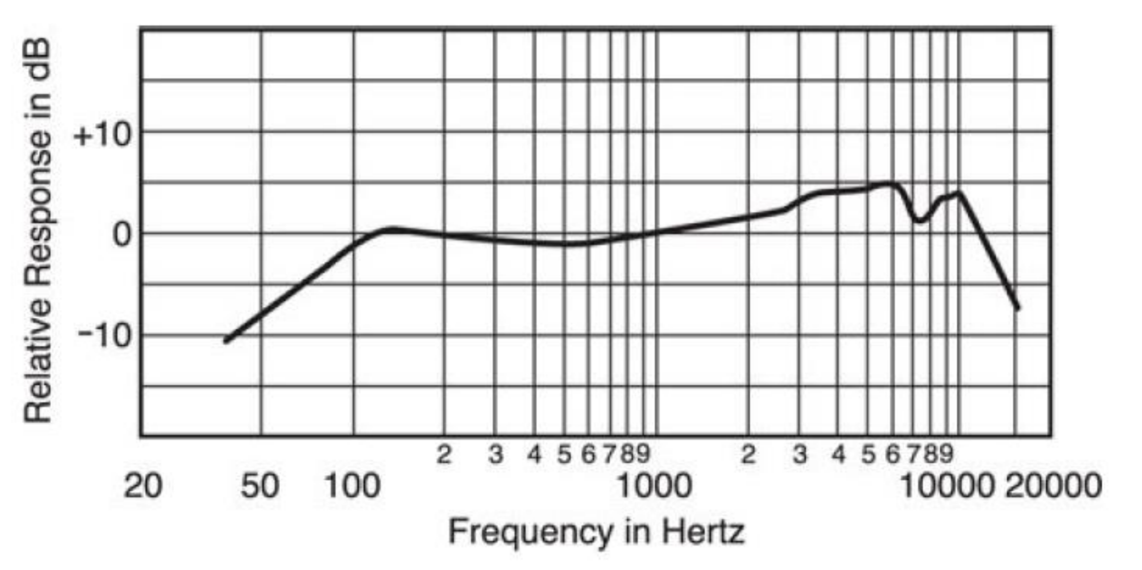
$$\left(\frac{x_m - O_x}{S_x}\right)^2 + \left(\frac{y_m - O_y}{S_y}\right)^2 + \left(\frac{z_m - O_z}{S_z}\right)^2 = g^2$$

Accelerometer is not alone…

- Other sensors can also be fingerprinted
- For example, the microphone

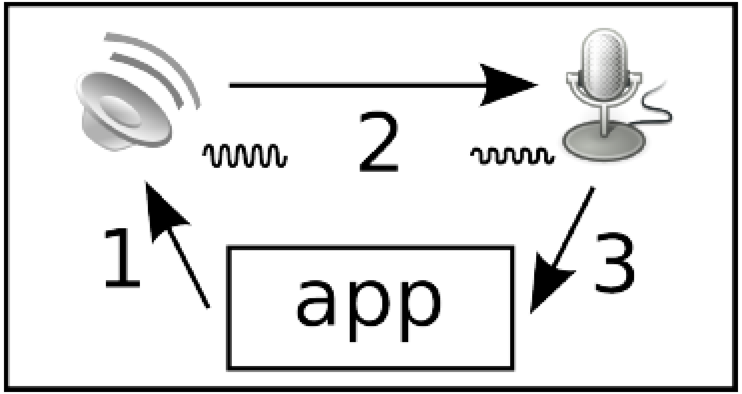
Microphone

- Each microphone has a characteristic frequency response curve

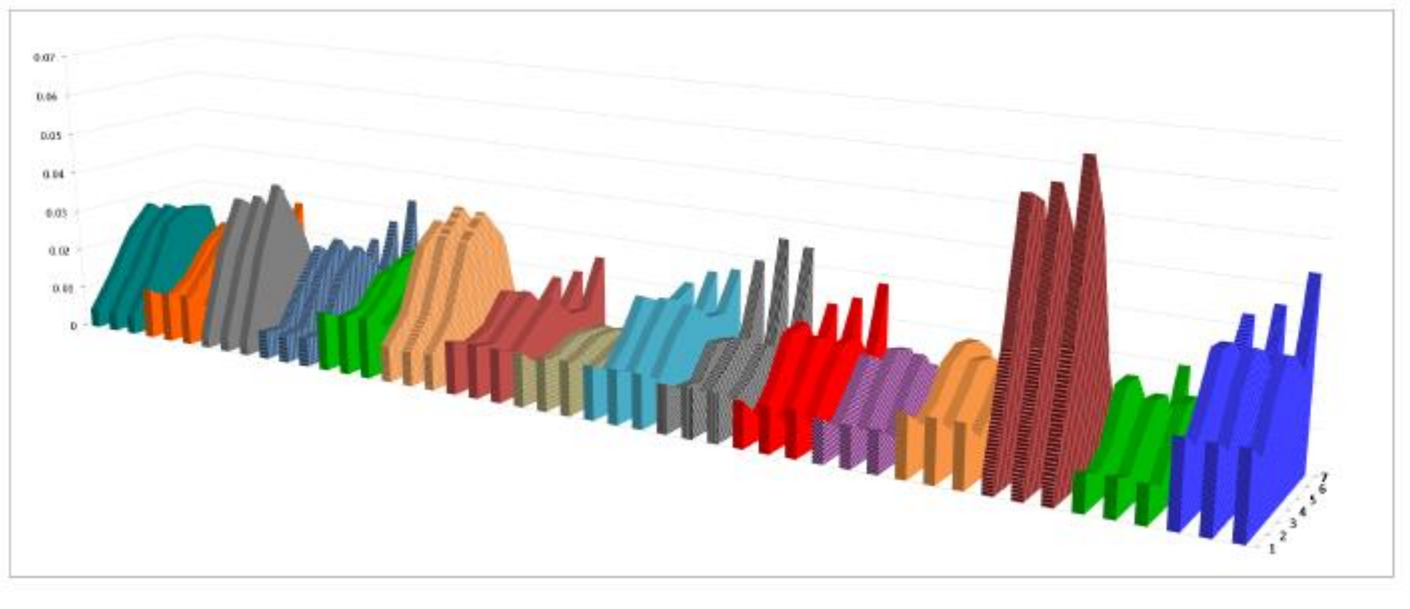


How can we fingerprint a microphone?

- We need some audio reference….
- We can use ….the phone's speaker



Experiment for 16 Motorola Droids

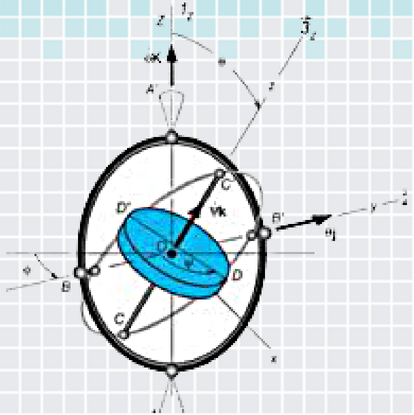


SendorID – Conclusions

- We have founds ways to construct a device ID by sensor fingerprinting.
- All the sensors' fingerprints may sum up to enough bits to identify all devices.
- It is hardware dependent.
- It can be used by web application.

RSAConference2015

San Francisco | April 20-24 | Moscone Center



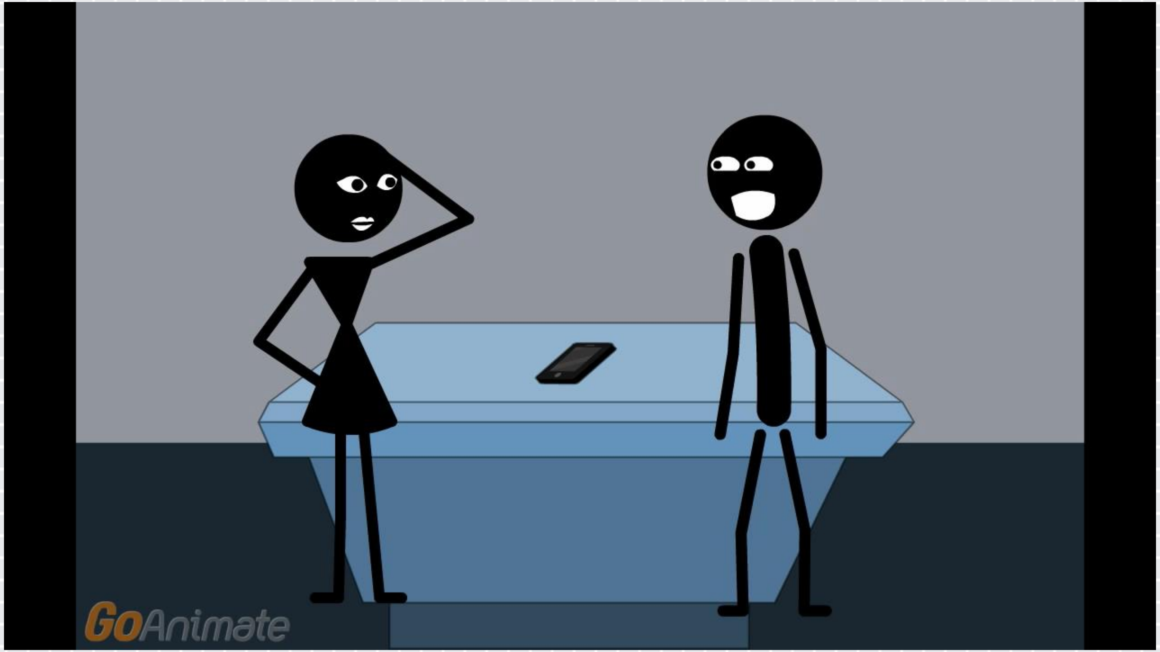
Gyrophone: Recognizing Speech from Gyroscope Signals

Y. Michalevsky, G. Nakibly and D. Boneh

#RSAC

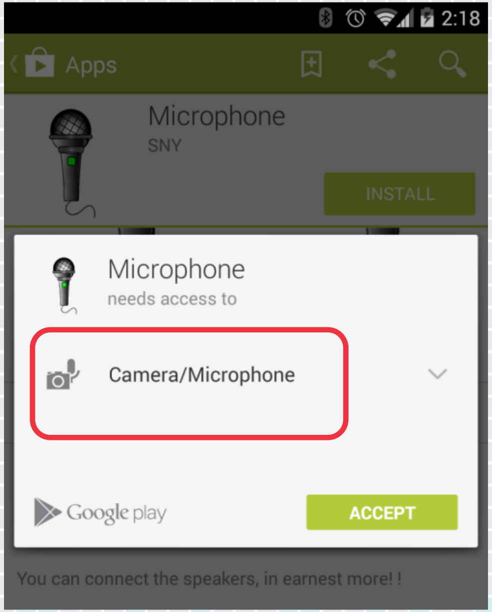
Scenario

People are talking in the vicinity of a mobile device

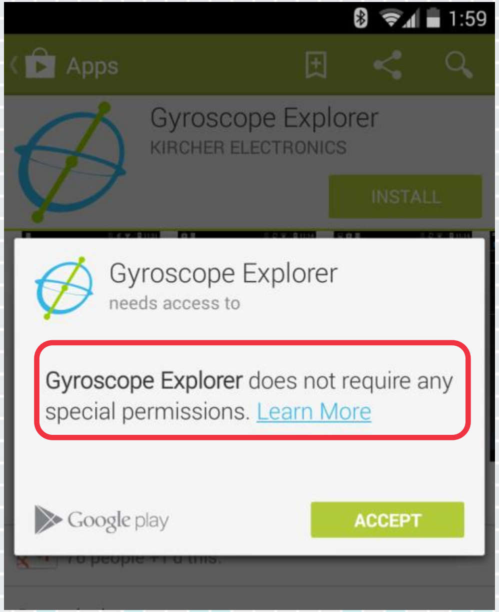


Microphone vs. Gyroscope Access

Requires permission

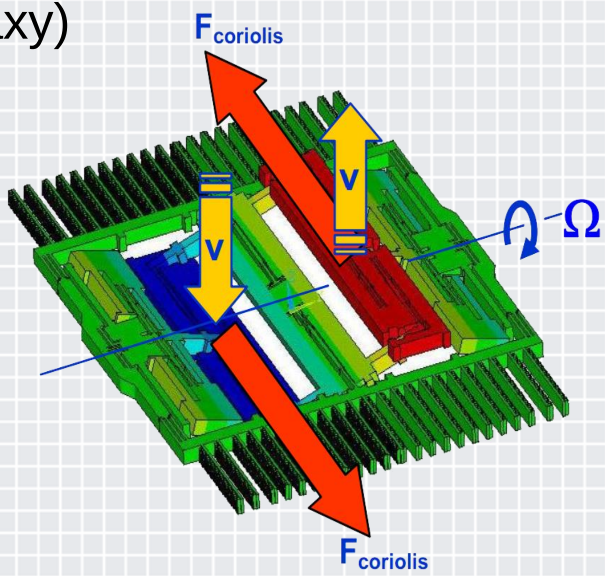


Does NOT require permission



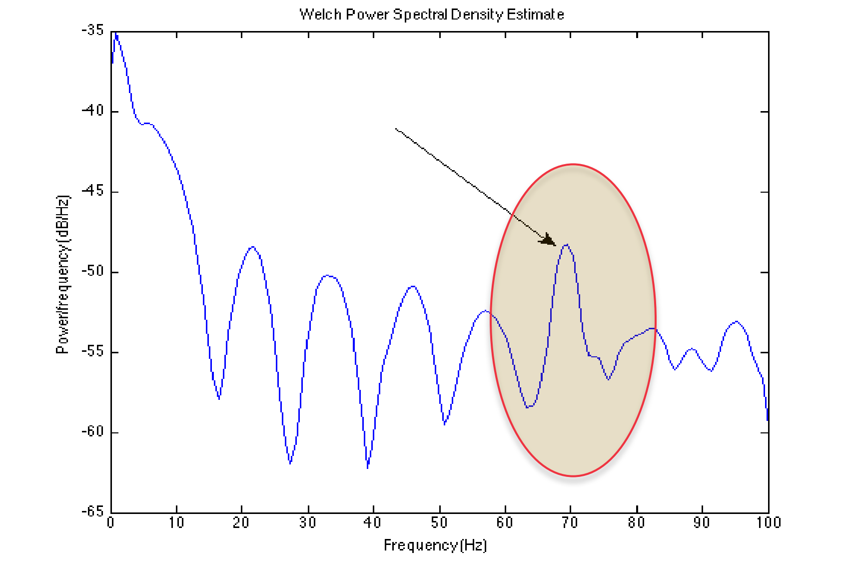
MEMS Gyroscopes

- Major Vendors:
  - STMicroelectronics (Samsung Galaxy)
  - InvenSense (Google Nexus)

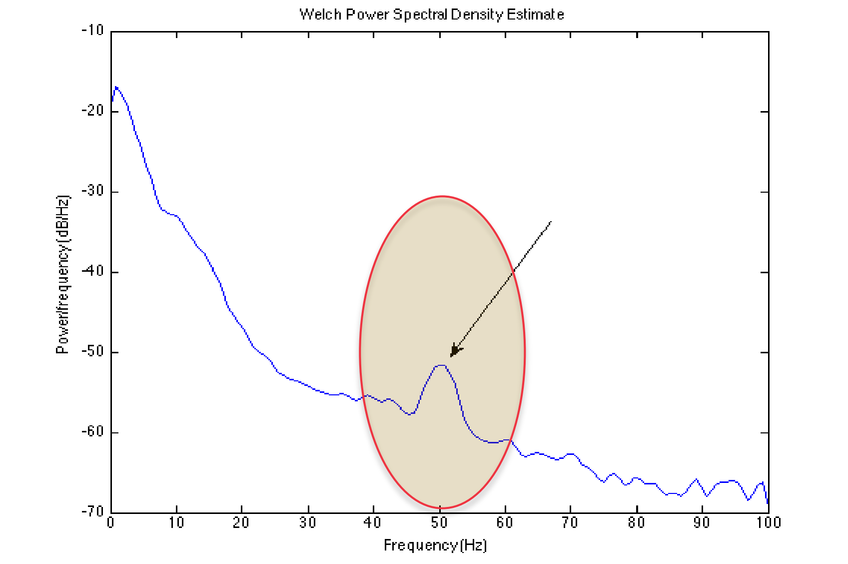


Gyroscopes are susceptible to sound

70 Hz tone PSD



50 Hz tone PSD



Gyroscopes are (lousy, but still) microphones

- Hardware sampling frequency:
  - InvenSense: up to 8000 Hz
  - STM Microelectronics: 800 Hz
- Software sampling frequency:
  - Android: 200 Hz
  - iOS: 100 Hz

- Very low Signal-to-Noise ratio (SNR)
- Acoustic sensitivity threshold: ~70 dB
  Comparable to a loud conversation
- Sensitive to sound angle of arrival
- Directional microphone (due to 3 axes)

Browsers allow gyroscope access too

WebKit based browsers
Gecko based browsers
Application

		Sampling Freq. [Hz]
Android 4.4	application	200
	Chrome	25
	Firefox	200
	Opera	20
iOS 7	application	100
	Safari	20
	Chrome	20

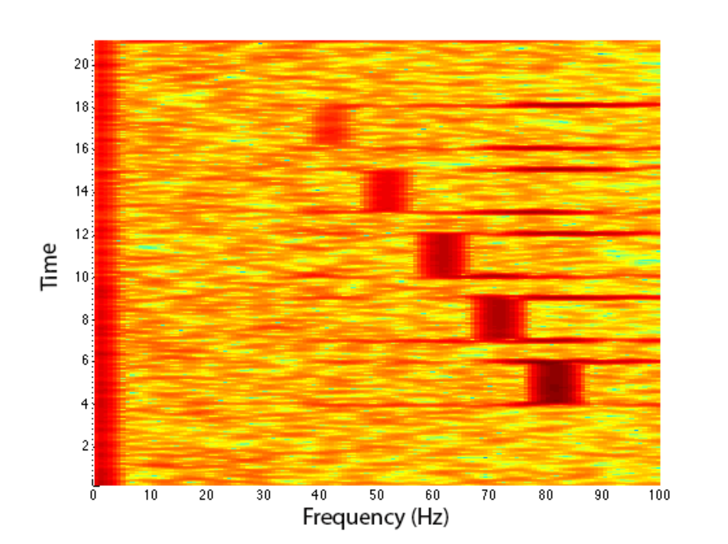
Problem: How do we look into higher frequencies?

Speech Range

Adult Male	85 – 180 Hz
Adult Female	165 – 255 HZ

We can sense higher frequencies signals

Due to aliasing



Recording tones between 120 to 160 Hz on a Nexus 7 device

Experimental setup

- Room. Simple Speakers. Smartphone.
- Subset of TIDIGITS corpus
- 10 speakers × 11 samples × 2 pronunciations = 220 total samples

Speech analysis using a single Gyroscope

- Gender identification
- Speaker identification
- Isolated word recognition
  - Speaker independent
  - Speaker dependent

We can successfully identify gender

Nexus 4	84%
Galaxy S3	82%

Random guess probability is 50%

A good chance to identify the speaker

Nexus 4	Mixed Female/Male	50%
	Female speakers	45%
	Male speakers	65%

Random guess probability is 20% for one gender, and 10% for a mixed set

Isolated word recognition (speaker independent)

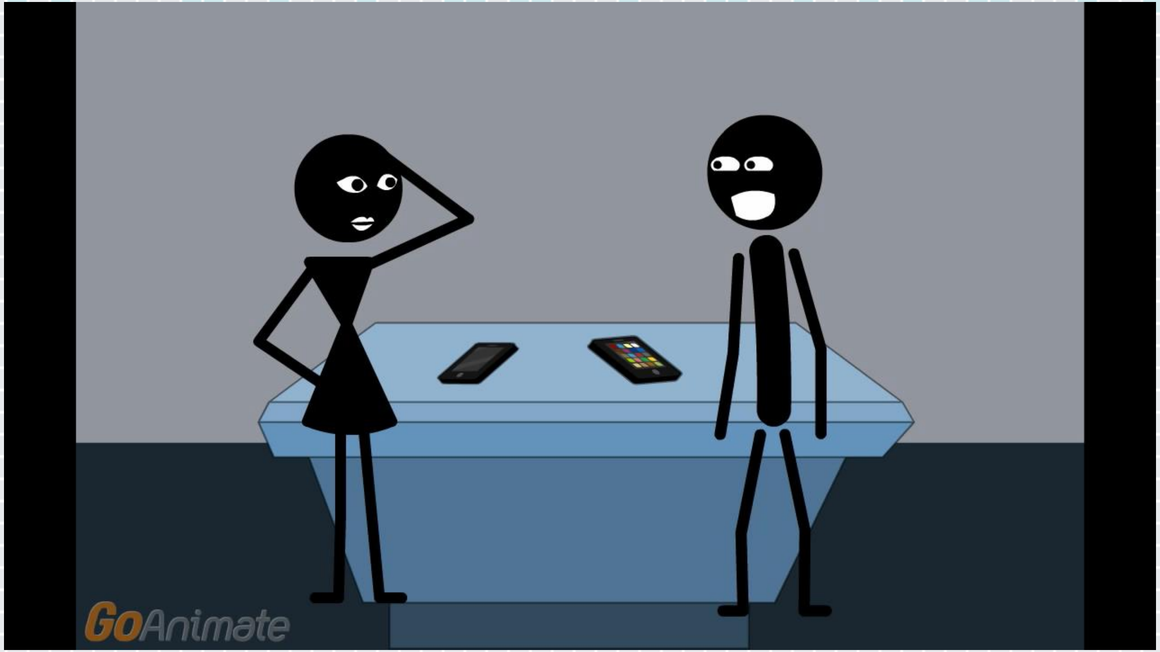
Nexus 4	Mixed Female/Male	17%
	Female speakers	26%
	Male speakers	23%

Random guess probability is 9%

Isolated word recognition (speaker dependent)

Nexus 4	Male speaker	65%

Random guess probability is 9%



Can we use multiple devices to improve the method?

Answer: Yes. Raising speaker dependent recognition rate to 77%.

Defenses

Software Defenses

- Low-pass filter the raw samples
- 0-20 Hz range might be enough for browser based applications (learning from Web-Kit's example)
- Access to high sampling rate should require a special permission
- Can possibly be applied by software providers / open-source community

Hardware Defenses

- Hardware filtering of sensor signals (not subject to configuration)
- Acoustic masking
- Can possibly be applied by vendors

More details can be found here

crypto.stanford.edu/gyrophone

To conclude

- We believe this is only the beginning
- Many more unexpected information leakages will be found in coming years.
- Treat every app you install as having ‘root’ on the phone!
- Now we know you will think twice before installing that “harmless” game ….

Questions?

- Yan Michalevsky – yanm2@cs.stanford.edu
- Gabi Nakibly – gabin@rafael.co.il