Analyzing Keyboard Vibrations

decoding keystrokes from nearby cell phone accelerometer data

John Harakas
Dept. of Mathematics and Computer Science
Faculty Advisor: Dr. Rosiene

Background Info (1)

- Data is digital pollution
  - Our phones *fart* personal information about us.
  - Information about our surroundings.
- Every phone has an accelerometer
  - Measures acceleration, used for tilting and rotation of screen on mobile devices.
  - Used in mobile games.
  - Used in apps to track how many steps you take in a day

Background Info (2)

- Data is as a by-product of computation
- Side Channel Attacks
  - Attack systems based on physical information
  - Power consumption, electromagnetic leaks, acoustic cryptanalysis.

Bruce Shchnier: *Data and Goliath*

Accelerometers as side channels

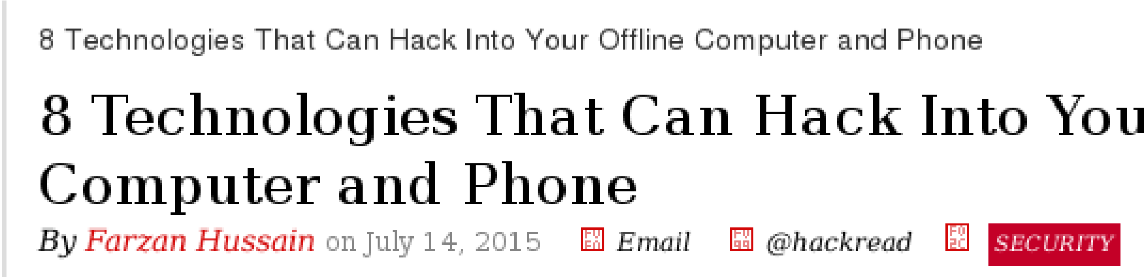
- They record info about your environment.
  - In Android, you don’t need to explicitly give an app permissions to access the phone’s accelerometer.
  - Malicious applications are *really* common.
- Record vibrations of nearby keyboard
  - Its not unrealistic to leave your phone on your desk while you are typing.

Accelerometers as side channels

- Bad actors will leave their phones next to you.

Google: “bad actor”

How Realistic is It?



8 Technologies That Can Hack Into Your Offline Computer and Phone

8 Technologies That Can Hack Into Your Offline Computer and Phone

By Farzan Hussain on July 14, 2015 Email @hackread SECURITY

How Your Smartphone's Accelerometer Could Uncover Your Passwords

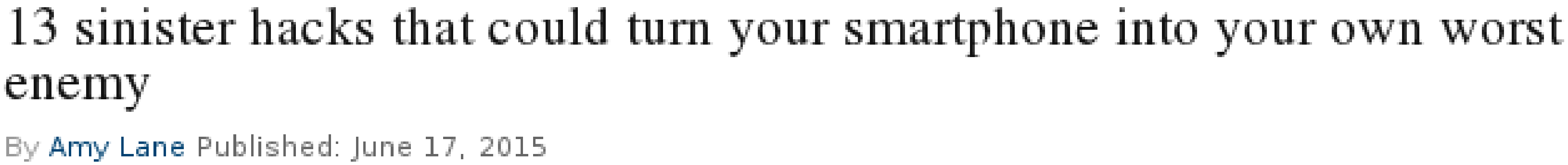
BY WESLEY FENLON ON OCT. 18, 2011 AT NOON

10 Ridiculous Ways Your Smartphone Can Be Used To Hack Your Personal Information

Vinay Devnath - 10th March 2016

5 Terrifying Smartphone Hacks You Won't Believe Are Possible

By Teddem Yee | July 22, 2013 | 1,915,004 Views



13 sinister hacks that could turn your smartphone into your own worst enemy

By Amy Lane Published: June 17, 2015

7 Ridiculously Cool Ways Your Phone and Computer Can Get Hacked

BY JAGADESH SIDDHARTHA · FEBRUARY 4, 2016

Previous Research

- Supervised learning based on acoustic dictionaries
  - Record lots of keystrokes and feed it through a neural network.
  - Doesn’t work outside of controlled conditions.
- Recognize key pairs
  - Vibrations of two keystrokes
- Only used the z-axis data

My Work

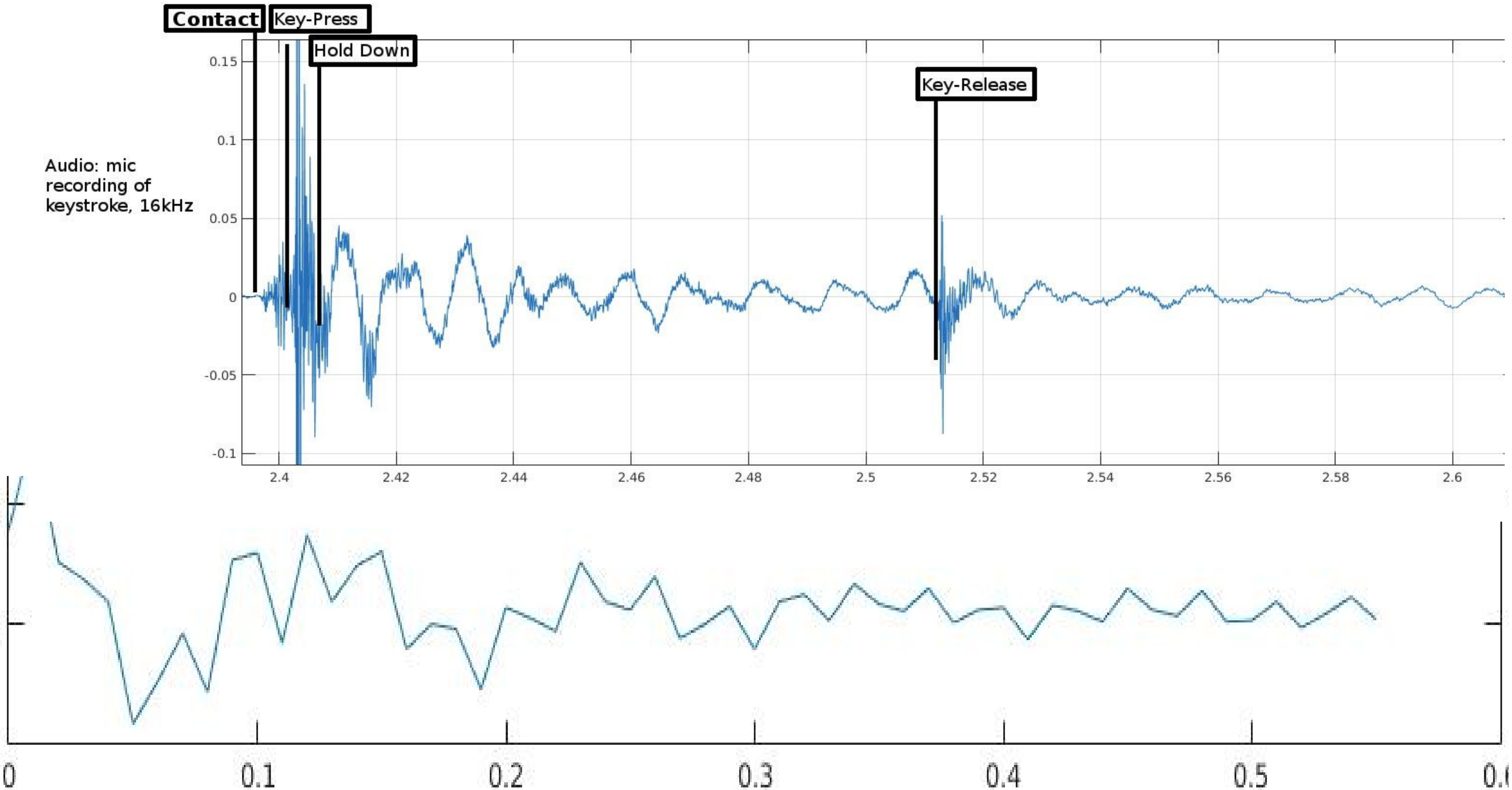
- Can keystrokes actually be uniquely identifiable?
- Can the x,y axes be used?
- Find traits that are independent of conditions
- Supervised learning (neural networks) is not robust
  - Extrapolating results when outside exact conditions
  - (spoiler) mixed results

What Makes This Difficult (1)

- Most phone accelerometers currently sample at 100Hz
  - Compare with phone microphone, thousands times faster
- Is a complex system, nonuniform
  - Do not type with consistent force each time
  - Each keyboard and surface is different.
  - Vibration travels from key, to the keyboard,
    to table, through table, to the device.
-

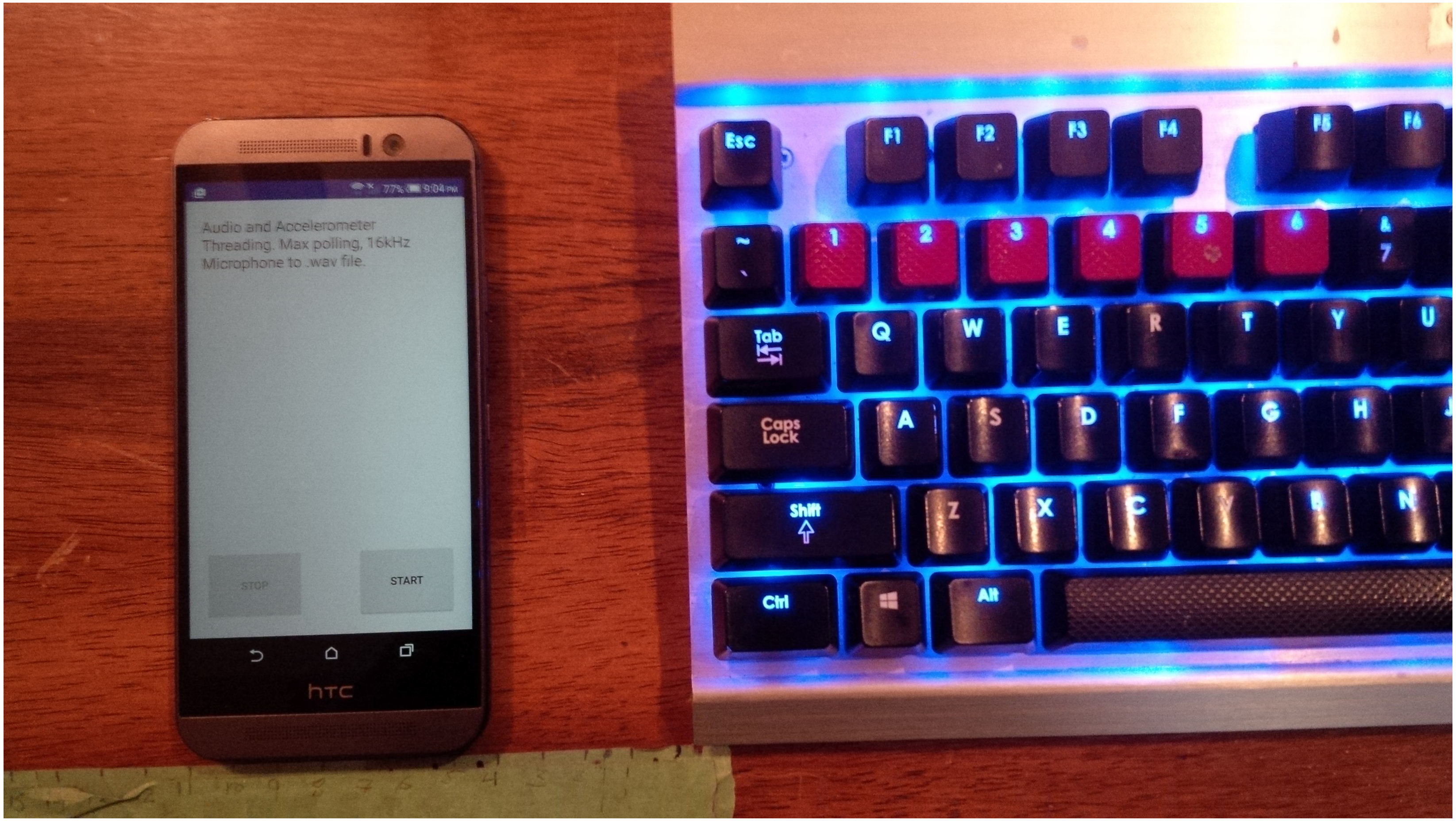
What Makes This Difficult (2)

- A single keystroke event is complicated:
  - Finger → Touch Key → Push Key → Hold Key Down → Lift Key Up → Untouch Key



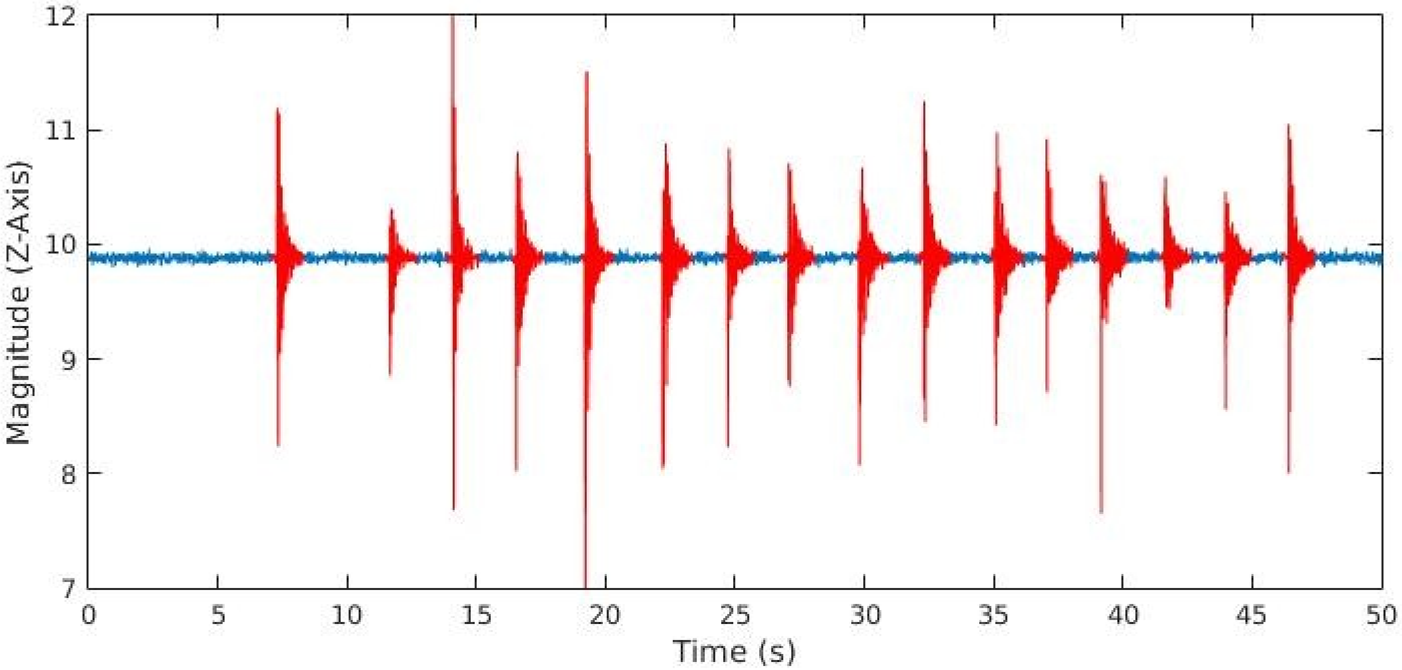
Experiment

HTC One,mechanical keyboard (more vibration) on wooden table
Recorded 4cm away (and other distances)

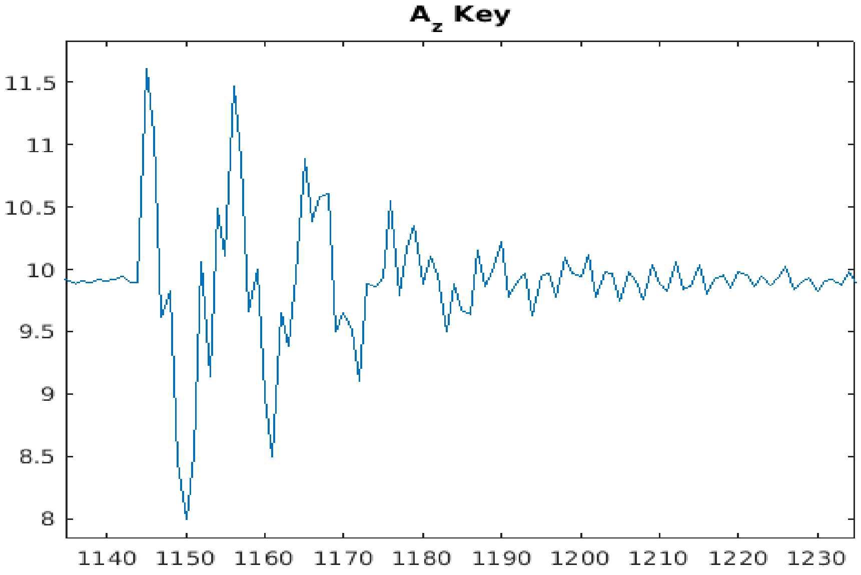


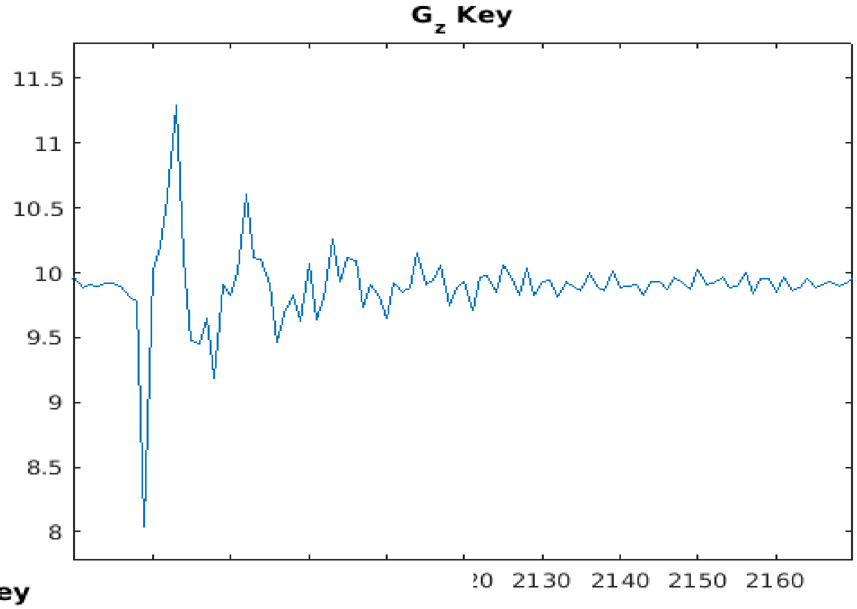
Methodology (2)

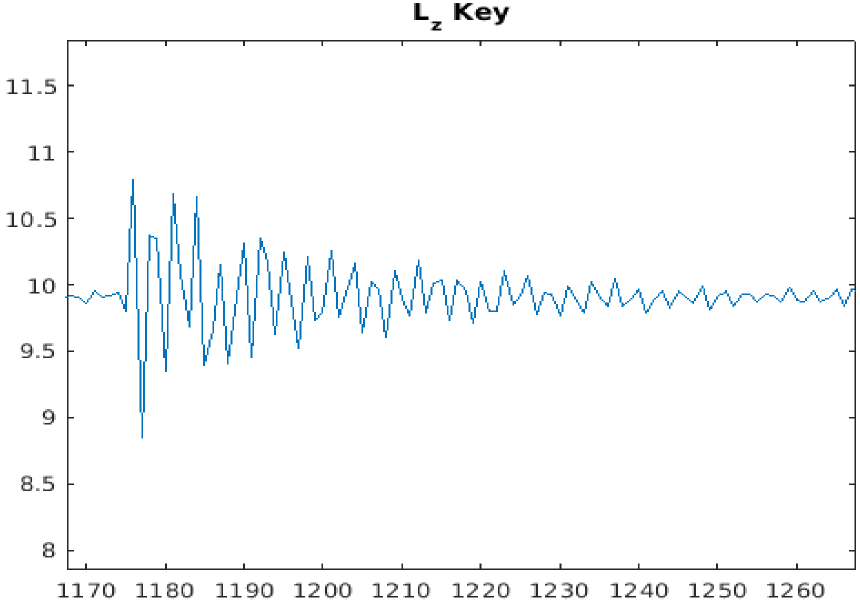
- Detect keystrokes
  - Transform, find peaks, threshold, etc...



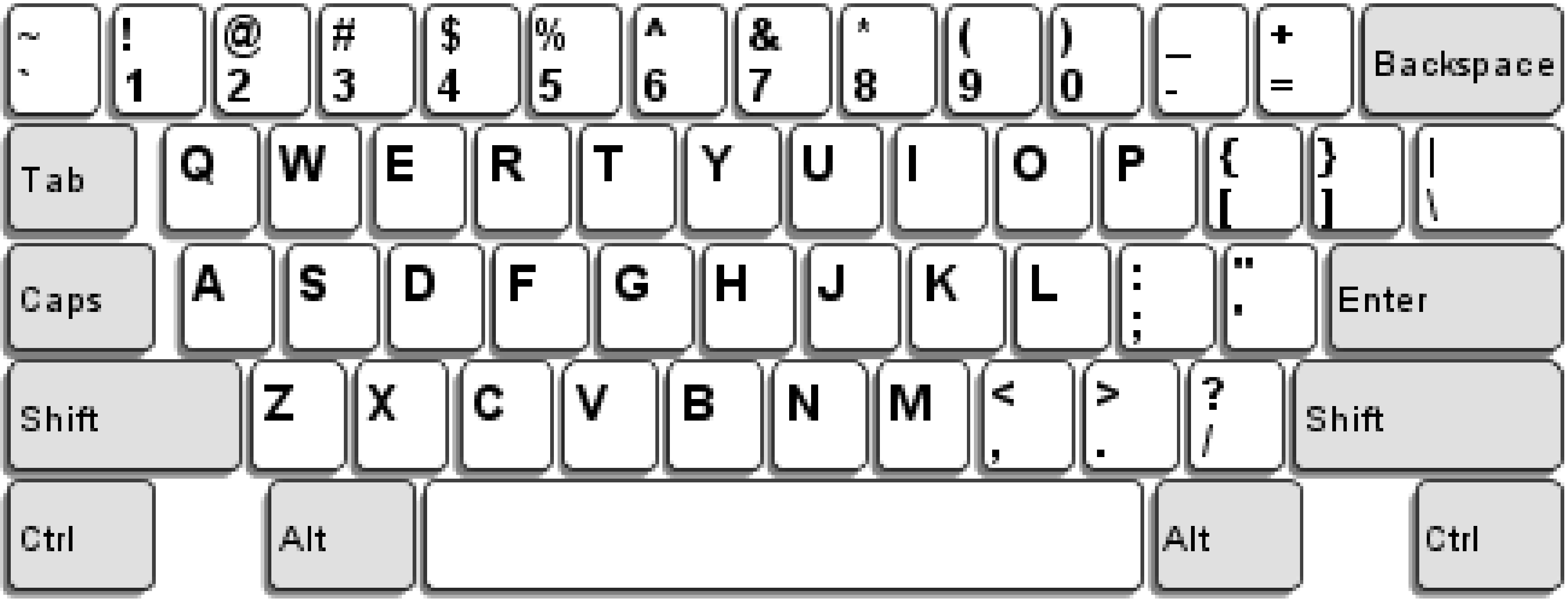
Everything Looks Like Noise







For reference

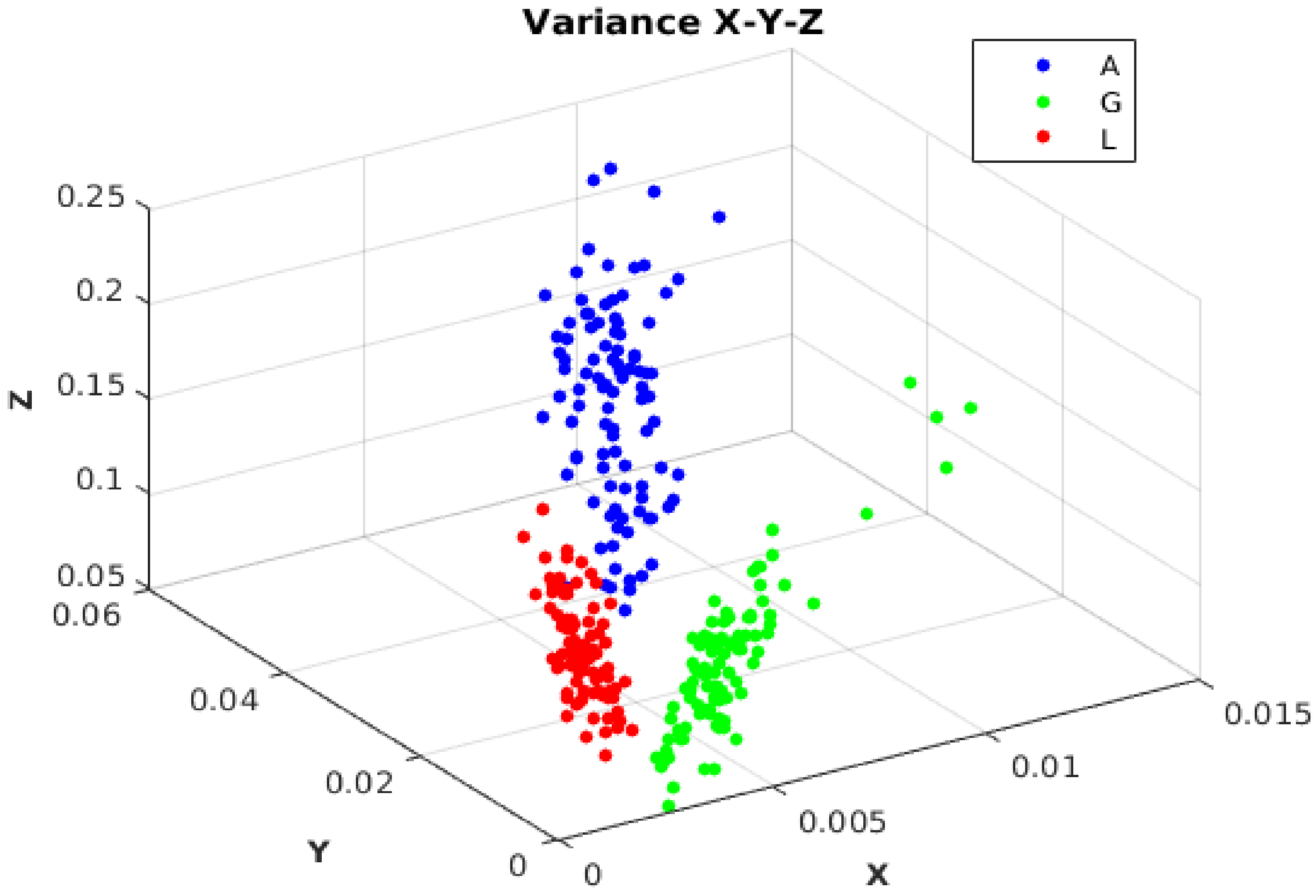


Some Features

- The measured frequency changes as the signal propogates through material
  - Mean frequency
- As vibration travels, amplitude diminishes, looks more like white noise.
  - Variance of signal: reflects noise

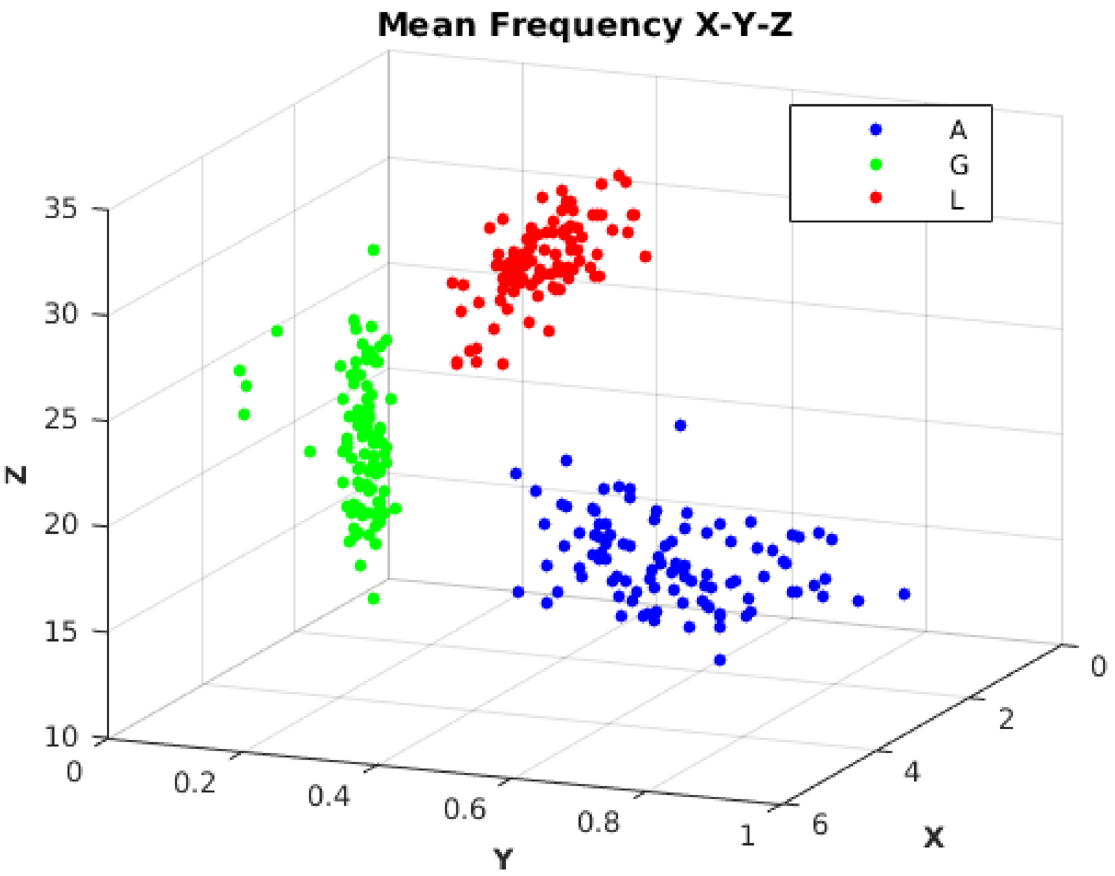
3D Components

- Variance



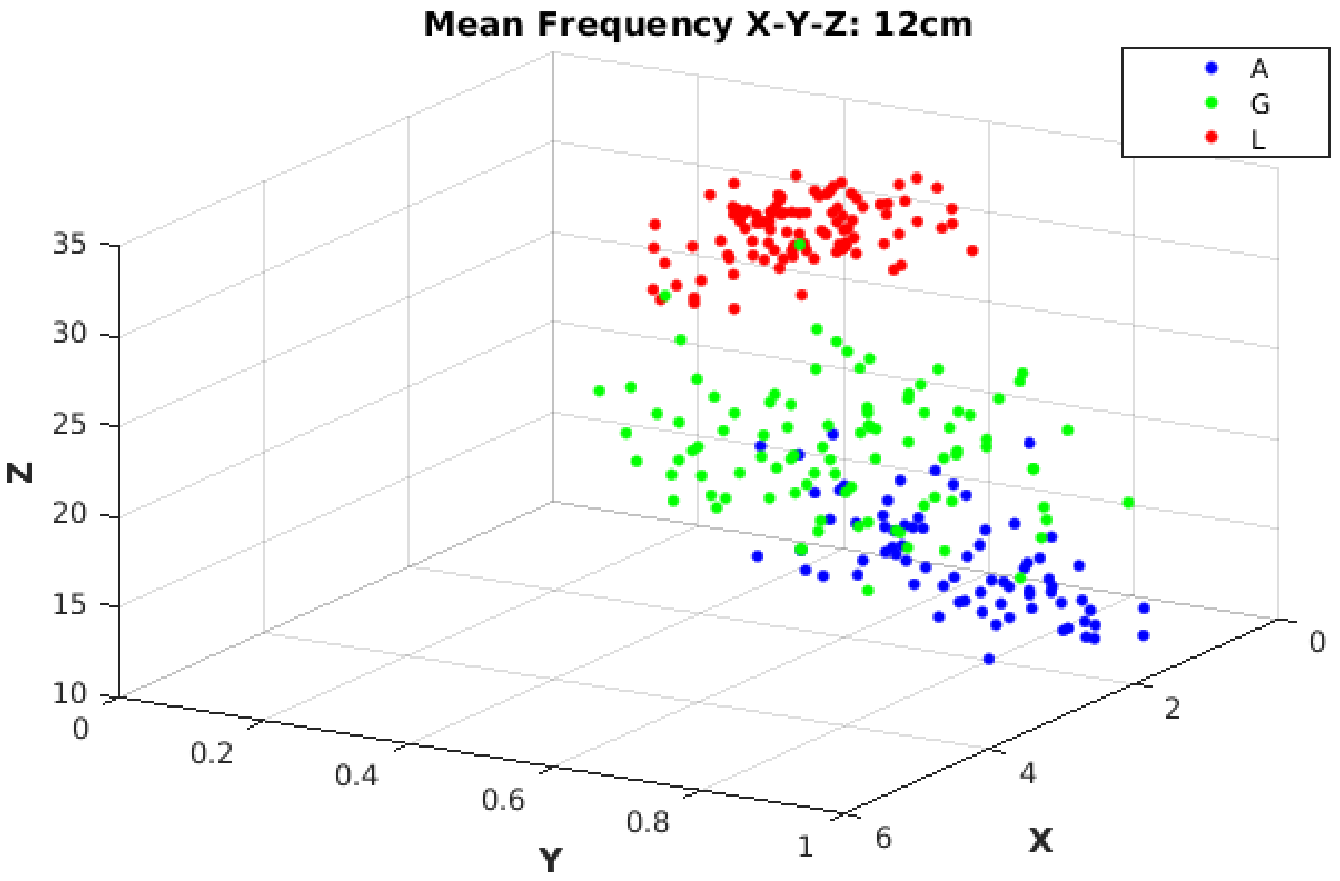
3D Components

- Mean Freq (4cm)



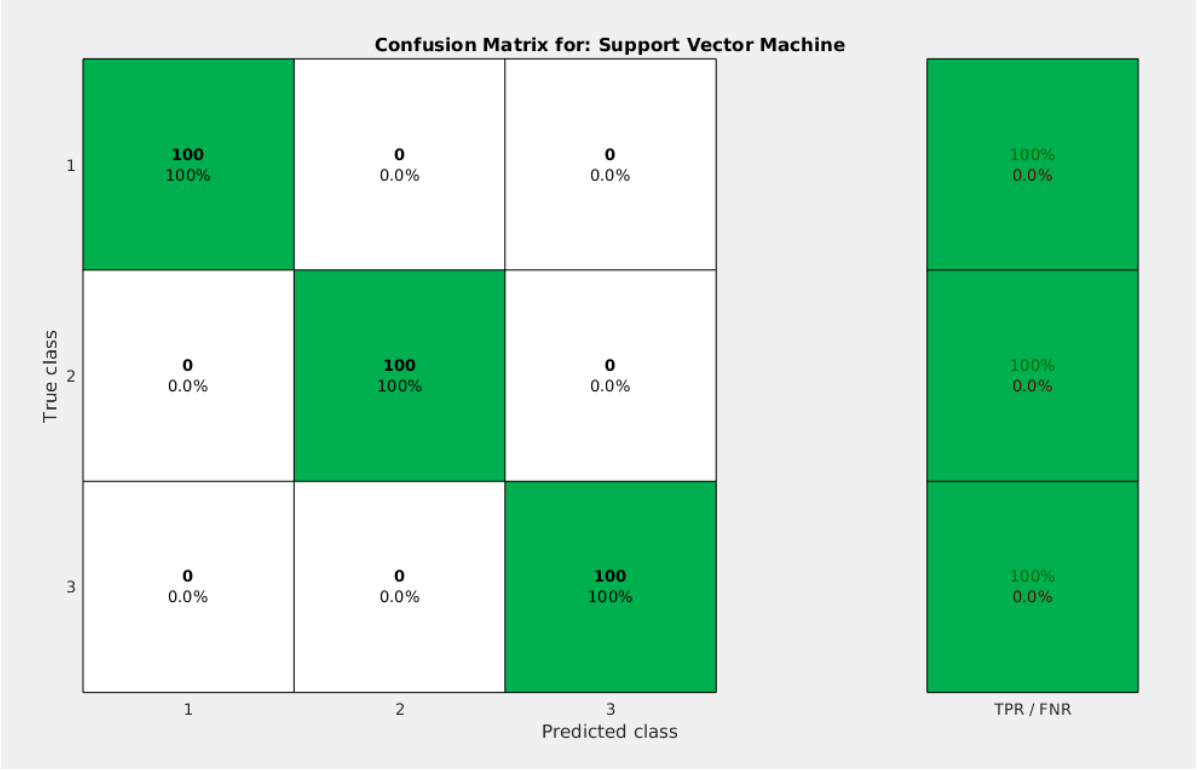
3D Components (12cm)

- Mean Freq (12cm)



3 Is Easy

- Easy classification for any unsupervised learner:
  - K nearest neighbor, linear support vector

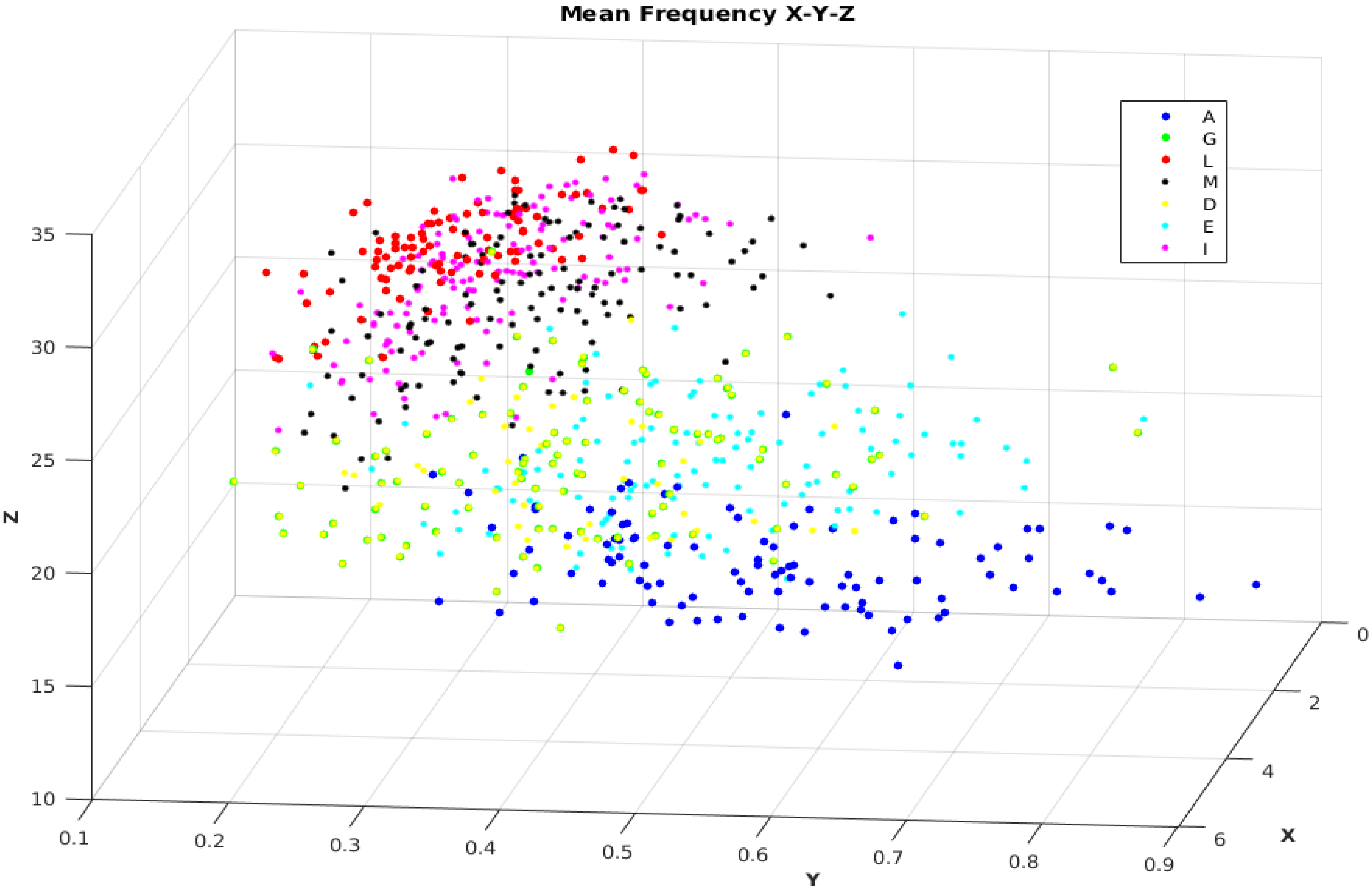


Confusion Matrix for: Support Vector Machine

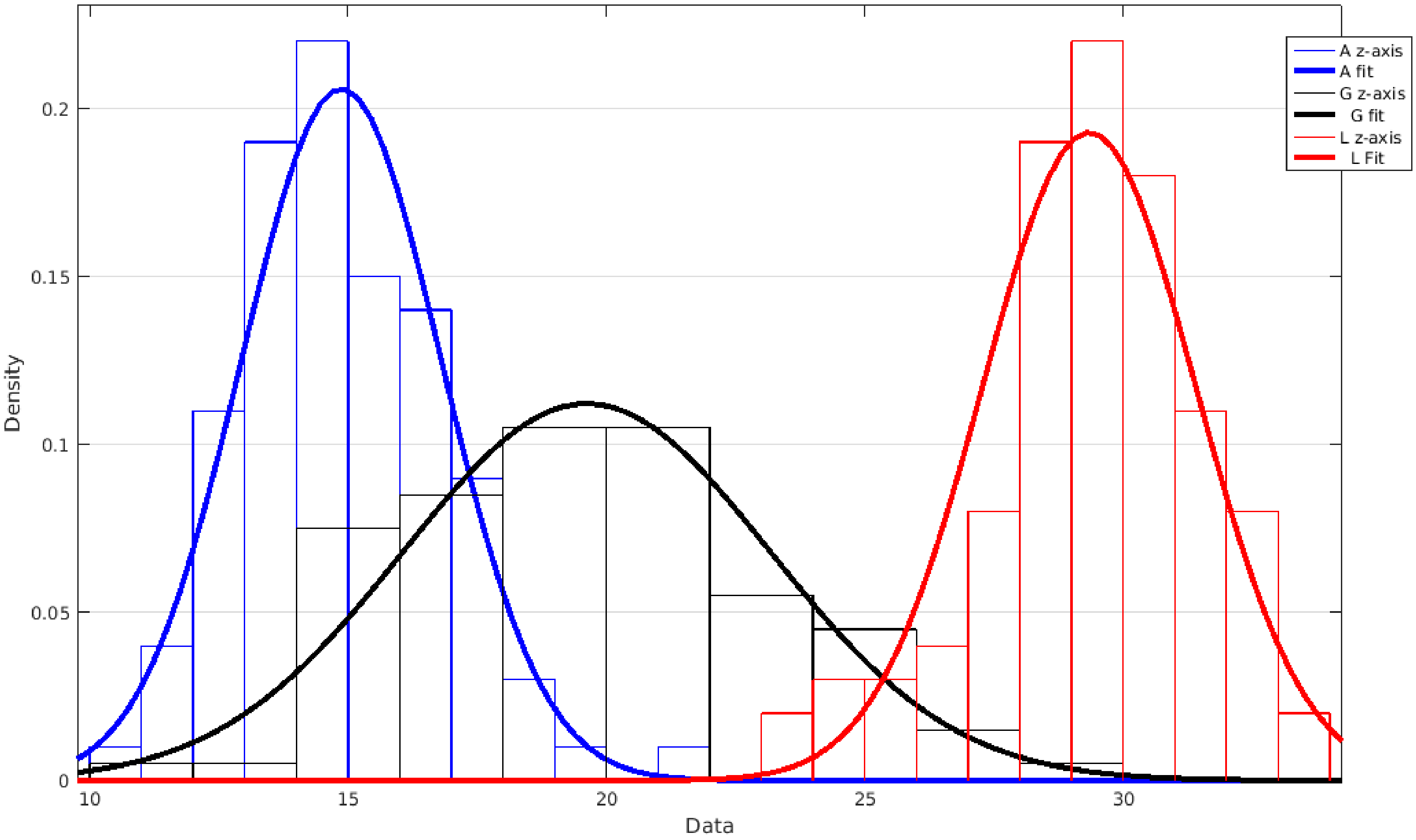
True class	1	2	3	TPR / FNR
1	**100** 100%	**0** 0.0%	**0** 0.0%	100% 0.0%
2	**0** 0.0%	**100** 100%	**0** 0.0%	100% 0.0%
3	**0** 0.0%	**0** 0.0%	**100** 100%	100% 0.0%

Predicted class

More is hard: Indistinguishable



Mean Freq is Normal



Better Filtering

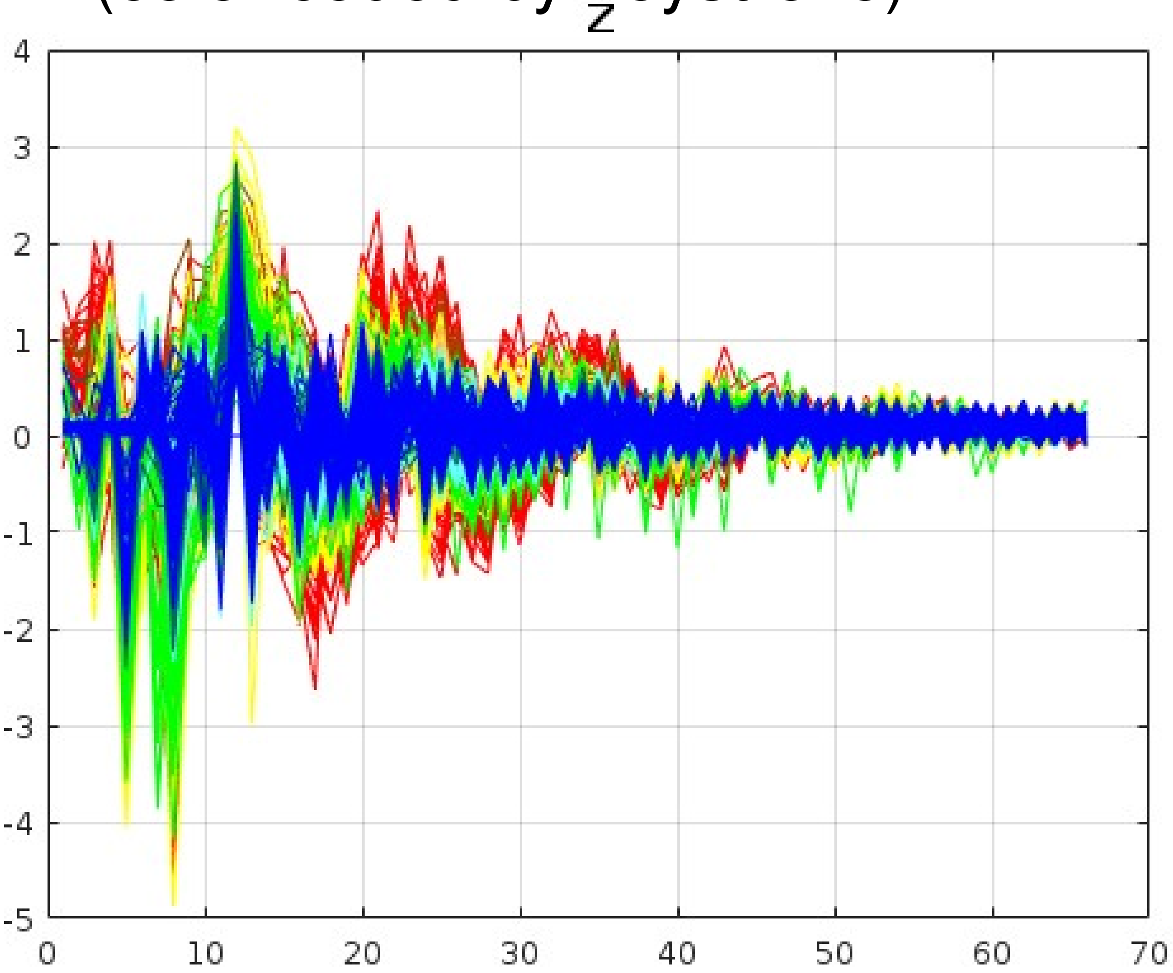
- 100Hz is low
  - Nyquist Sampling Theorem, need to sample at least twice the frequency of the signal
  - High frequency vibration not being measured correctly
  - Signal aliasing (overlapping higher freq signals)

Better Filtering

- Lowpass filter before acquisition
  - Reject higher frequency samples
- Matched filter, optimal linear filter
  - Like a template
  - Keystroke = Signal + Noise
  - Min noise ? Max Signal-to-Noise ratio

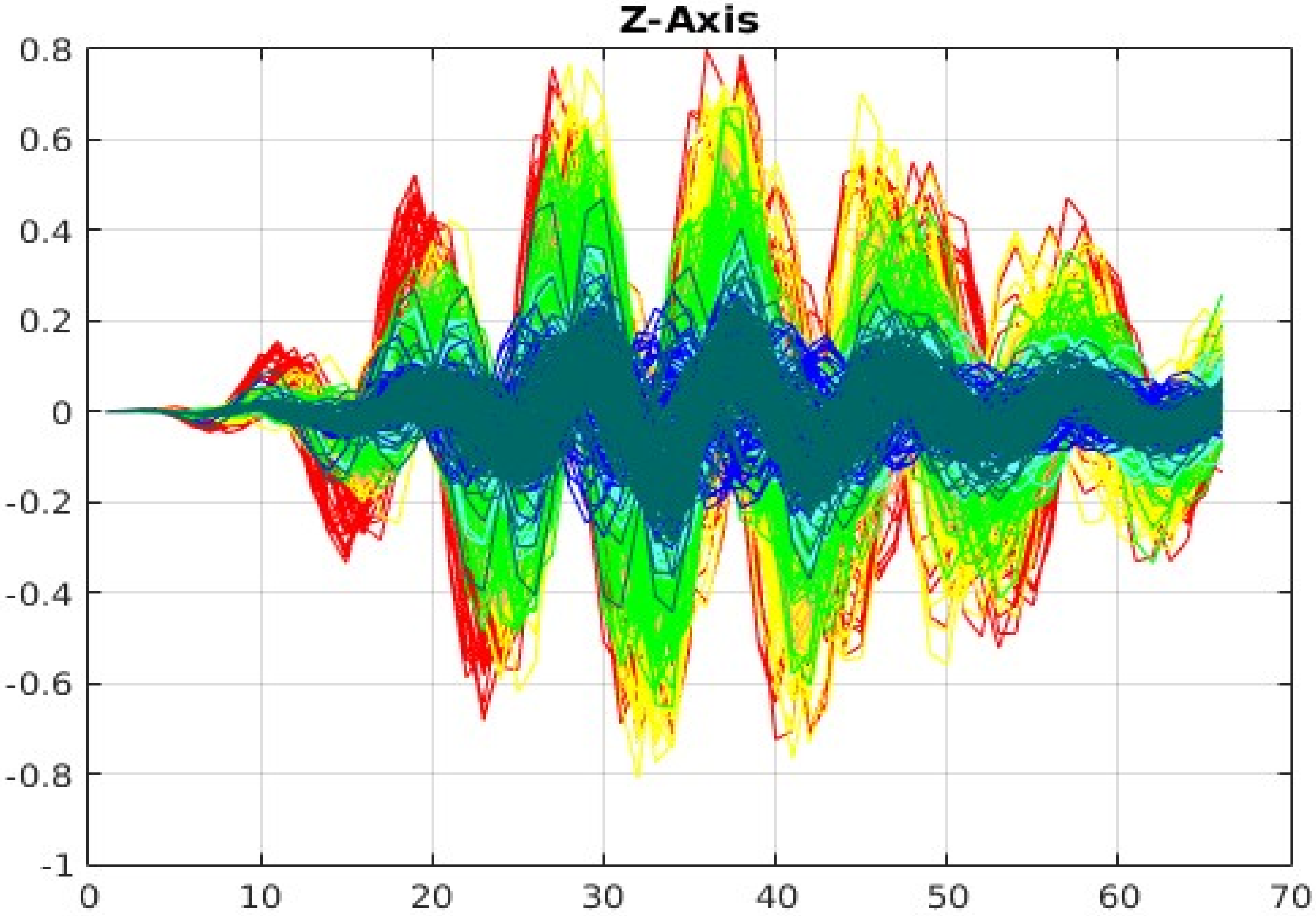
Filtering: None

Signals are indistinguishable,
(color coded by keystroke)



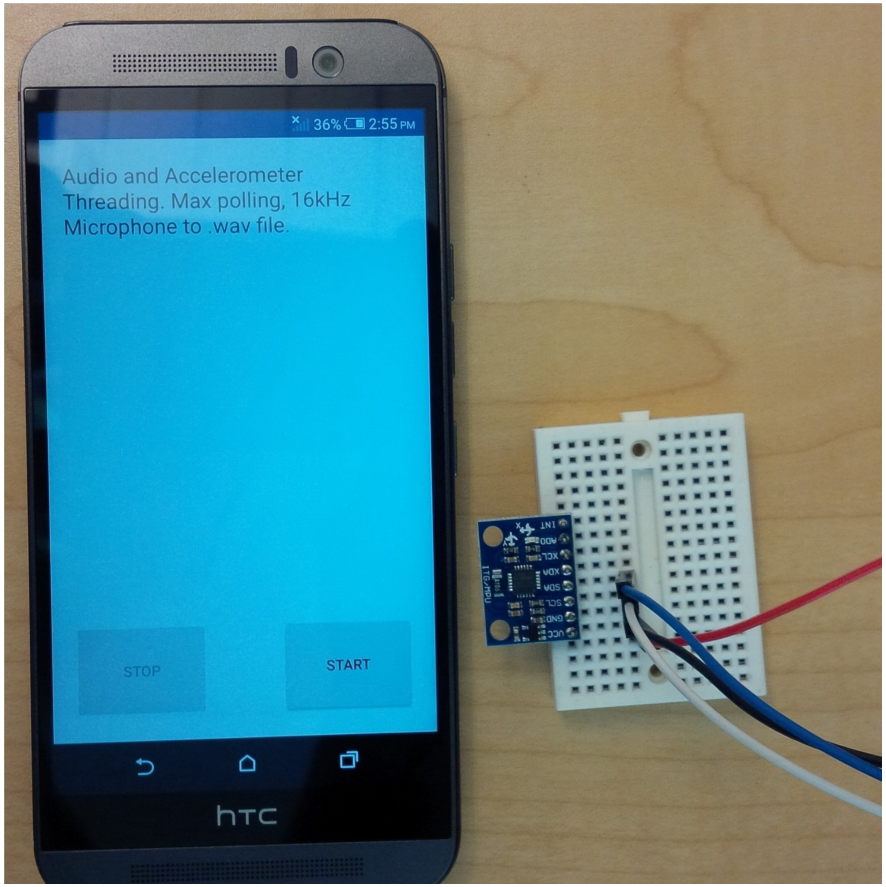
Filtering: Bandpass

- Bandpass Filter, cut out lower and upper frequencies
- More distinct



More Sampling

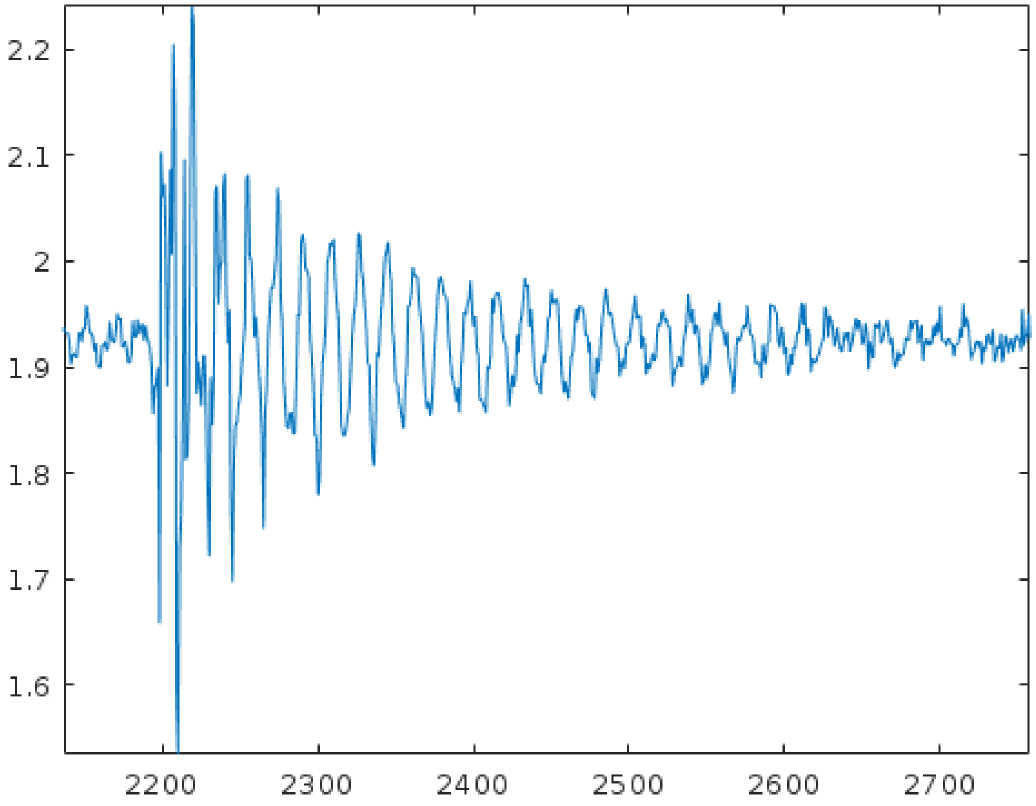
- MPU-6050 sensor module
  - 1kHz(max) Accelerometer (10x faster)

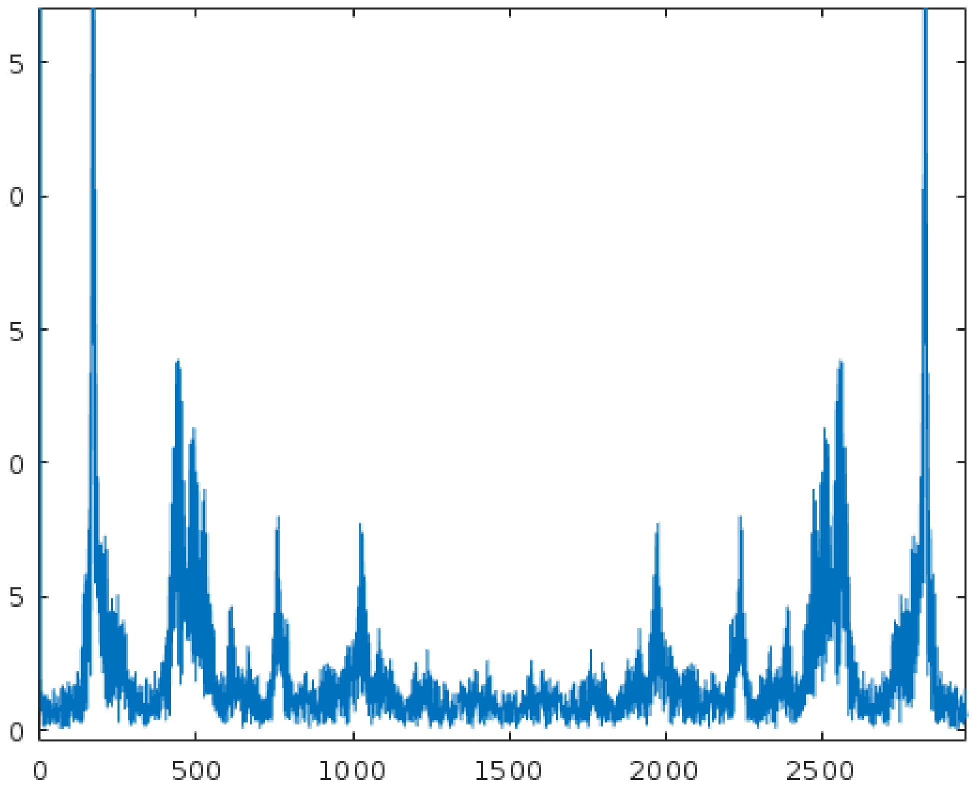


Audio and Accelerometer Threading. Max polling, 16kHz Microphone to .wav file.

More Problems

- The phone weight acts as a dampening mechanical lowpass filter
- Sensor chip is too light, responds to high frequency noise
- More aliasing amongst higher sampling.





Bigger Picture

- This can be solved with weighing down the sensor, set a lowpass at the hardware level
- The goal is not to reconstruct the signal
  - Only need to discriminate between keystrokes
- Discriminating Left/Right/Center keys and knowing the word length significantly reduce password search strategies in of itself.

Bigger Picture

- Mean frequency and the signal variance are not specific to an exact environment
  - Variance reflects the signal power. A lower variance indicates attenuated signal.
- More robust than an acoustic dictionary
- Other statistical methods can be supplemented
  - The unknown signal could be a vowel.

Future Work

Better filtering

- Sensor fusion
  - Combine with other sensors
  - Gyroscope, microphone
- Put it all together
  - Implement all aspects as one program

Concluding Remarks

- Realistically will this happen to you?
  - Probably not (for now)
- Sensors are getting better, faster, stronger
  - $5 online, size of thumbnail

Questions.
Remarks.