Embedded Security

EECE 5698-08: Special Topics: Cyber-Physical Security of IoT Systems in the Age of AI

Lecture 3: Signals and Systems Refresher

Prof. Kevin Fu

September 15, 2025

https://spqrlab1.github.io/emsec/

Last Time: Threat Modeling

- What?
  A systematic approach to identify, prioritize, and mitigate security risks
- Why?
  Prevents and reduces surprise of security vulnerabilities
- How?
  Attack trees, STRIDE, etc.
- When?
  Incorporate it early and iteratively in your projects

Today's Learning Goals

- Refresher on signals and systems intuition
- Ideation time for essay #1

Cardiac Rhythm Signals (time domain)

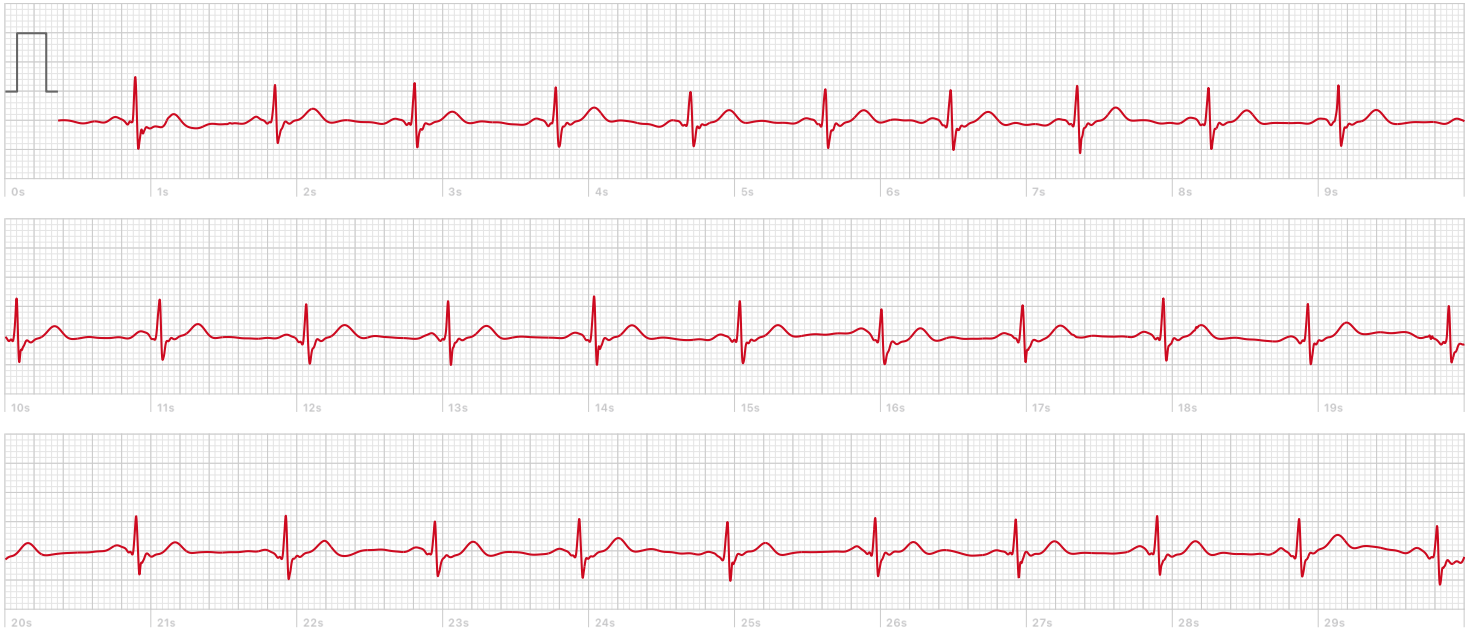
Kevin Fu

(Age 49)

Recorded on Sep 15, 2025 at 11:04 AM

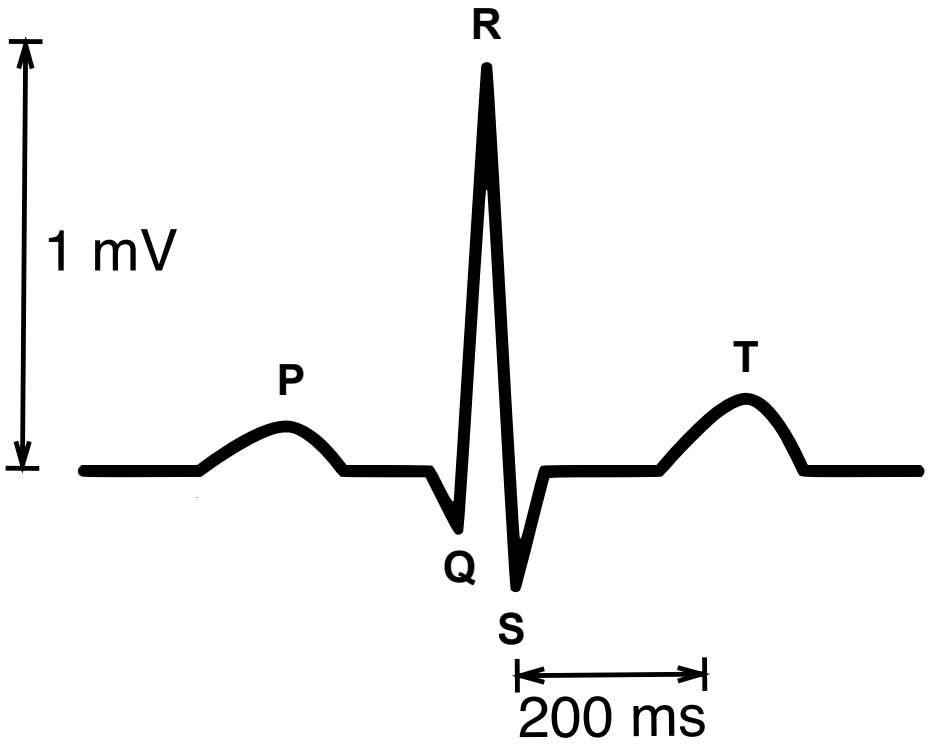
Sinus Rhythm — ❤️ 62 BPM Average

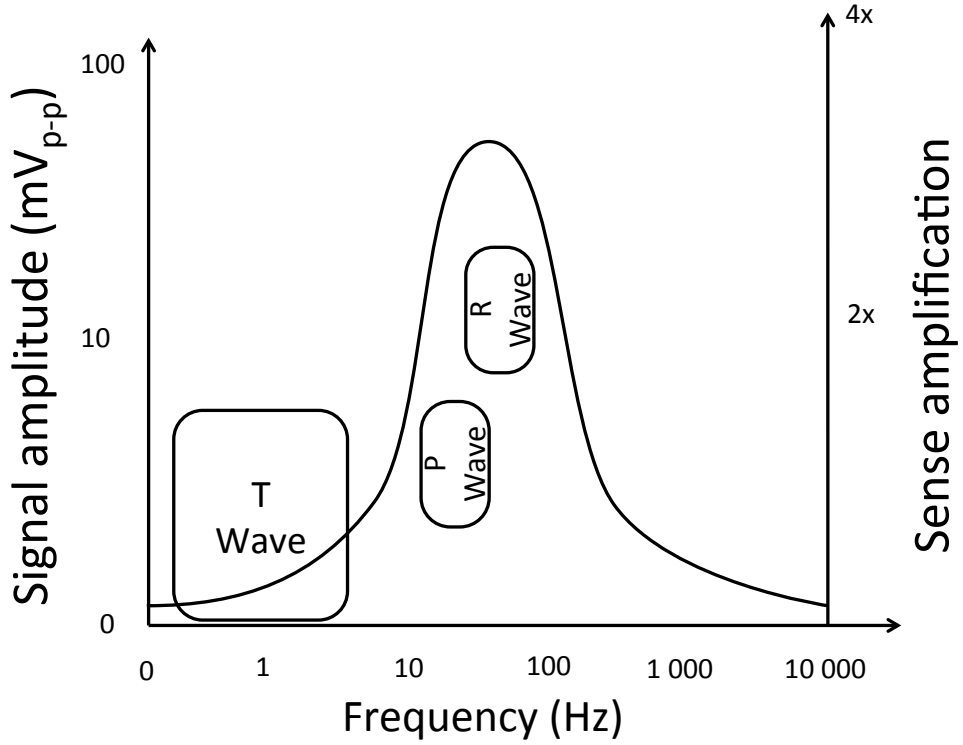
This ECG does not show signs of atrial fibrillation.



25 mm/s, 10 mm/mV, Lead I, 512Hz, iOS 18.6.2, watchOS 11.6.1, Watch7,9, Algorithm Version 2 — The waveform is similar to a Lead I ECG. For more information, see Instructions for Use.

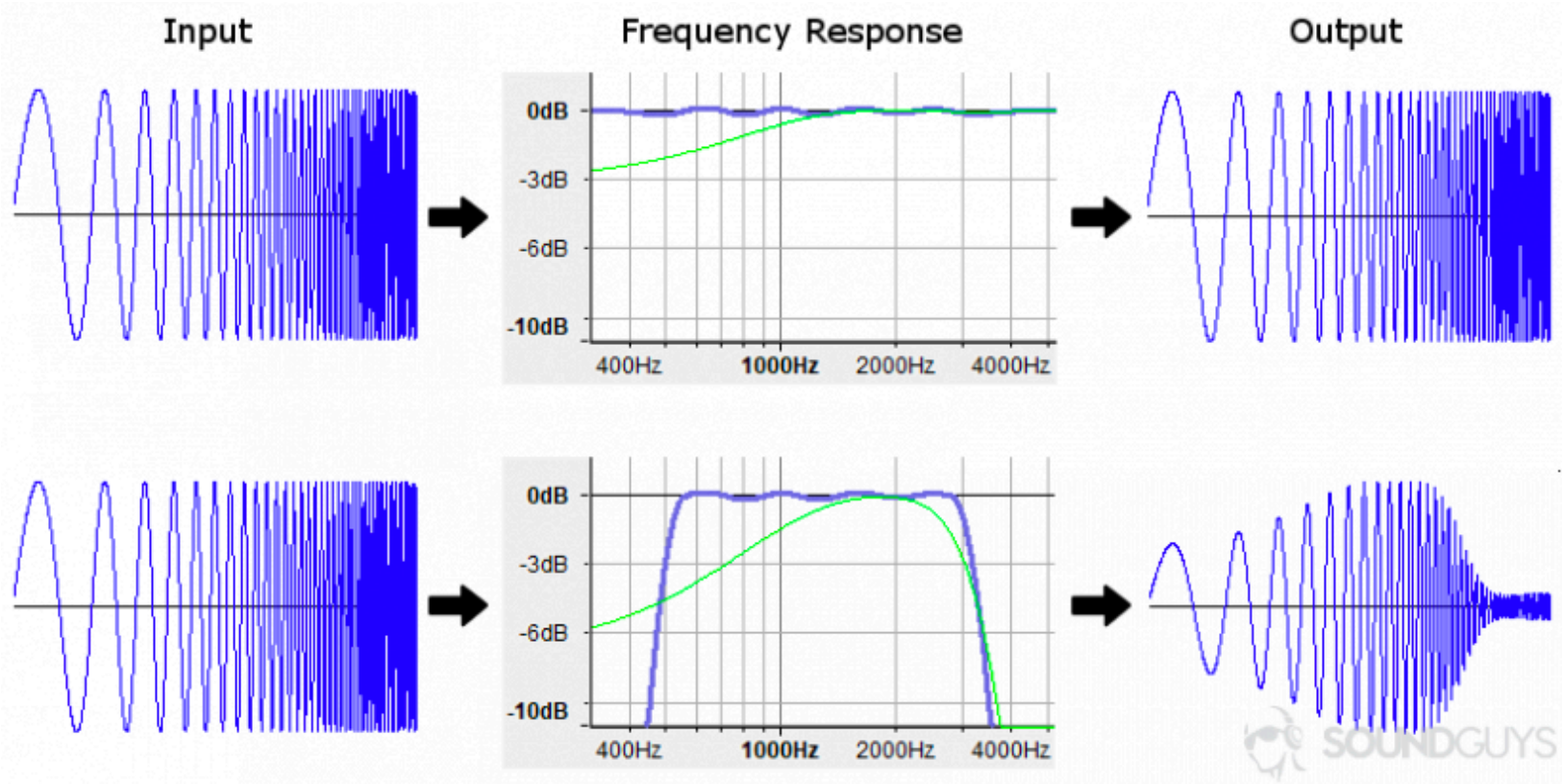
Cardiac Rhythm Signals (frequency domain)





Cohan et al, 2008

Frequency Response



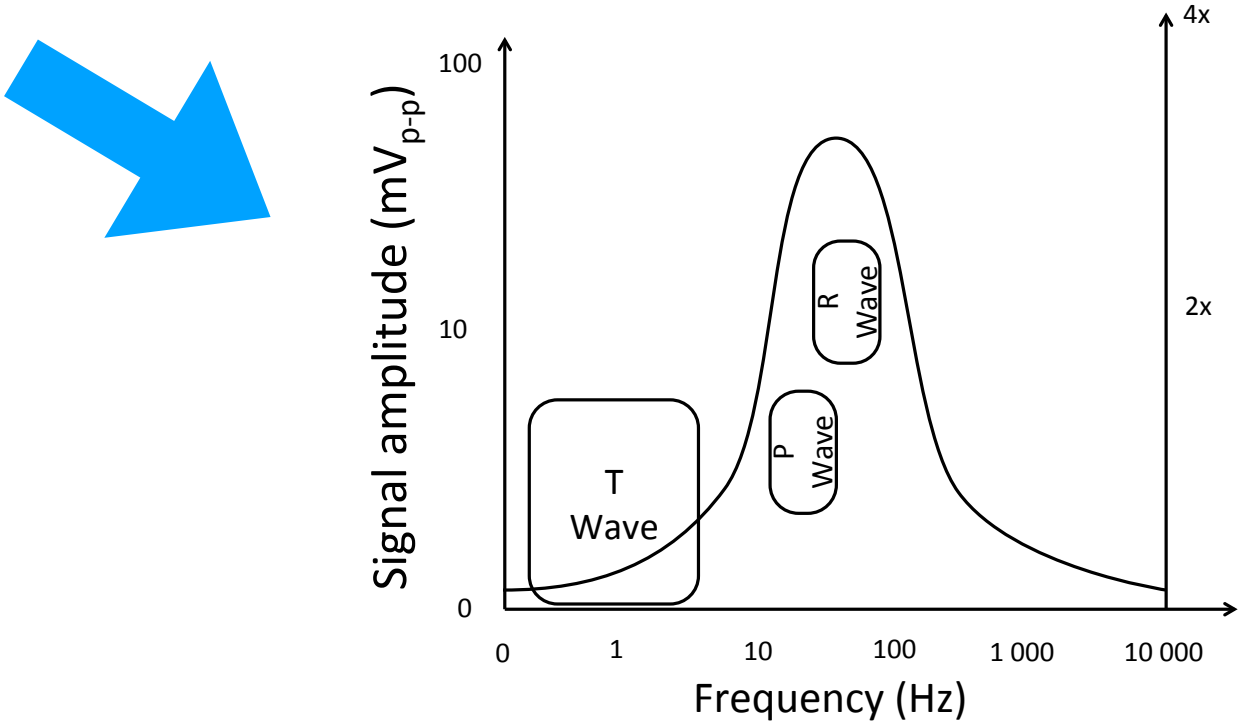
You will often hear a desire for a "flat" frequency response for an ideal reproduction of a signal. An ideal speaker or microphone would have a flat frequency response, but no device is perfectly flat in frequency response, which is why you ought attend to lecture in person to hear the secret exam clues from the 3rd order harmonics.

https://www.soundguys.com/frequency-response-explained-16507/

Frequency Domain Intuition

- Peaks = “ingredients" of signals

25 mm/s, 10 mm/mV, Lead I, 512Hz, iOS 18.6.2, watchOS 11.6.1, Watch7,9, Algorithm Version 2 — The waveform is similar to a Lead I ECG. For more information, see Instructions for Use.



Time Domain → Frequency Domain

- Sine wave in time domain = oscillation
- Frequency domain = spike in Fourier Transform
- Demo real-time spectrograms aka waterfall plots

Common Signal Filters

Low-pass, high-pass, band-pass, band-stop/notch

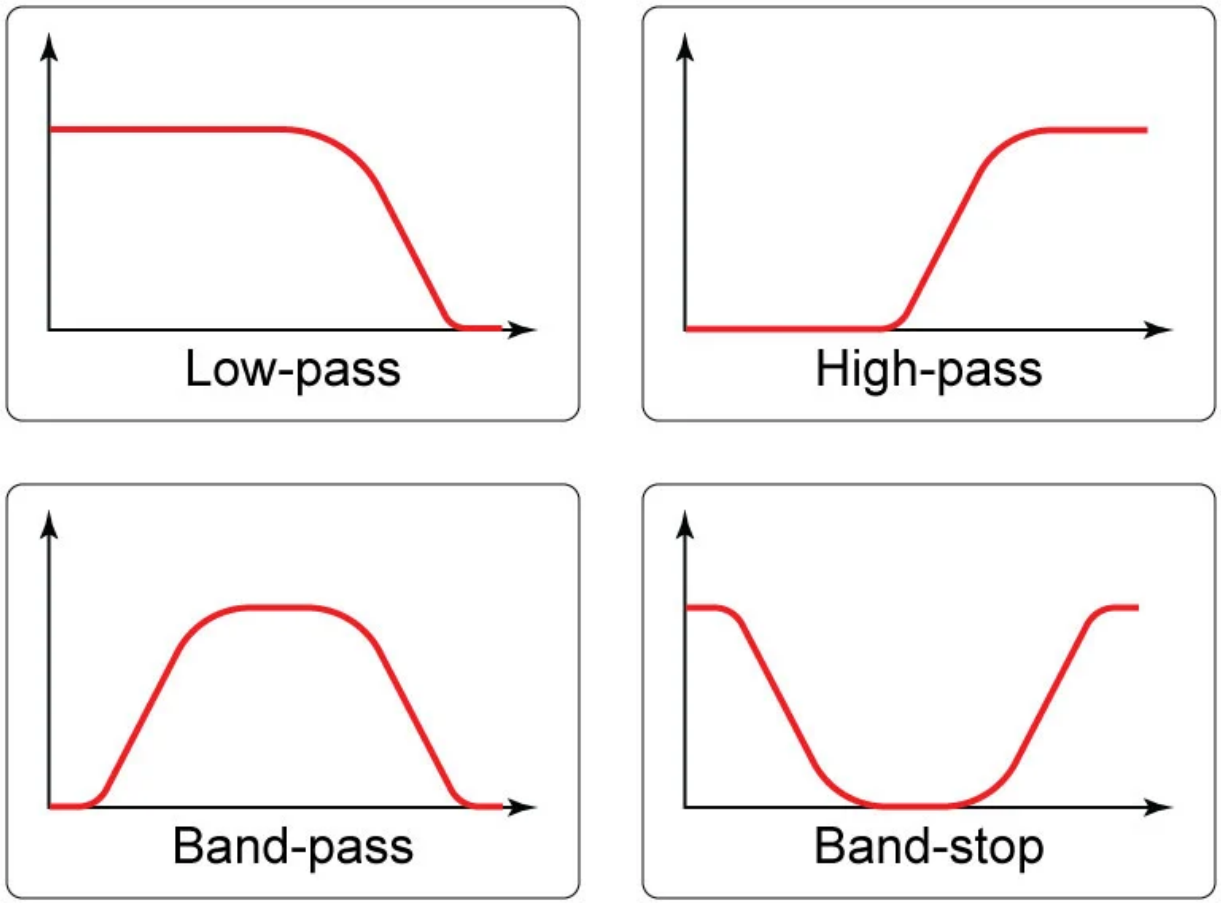
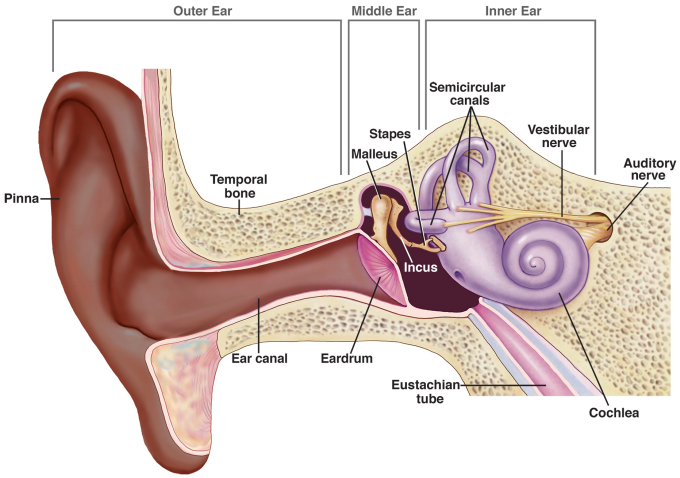


Photo credits: allaboutcircuits.com

Exercise: Filter Examples

Hearing



Laser Safety Goggles

FM Radio Tuner

90.9 wbur
BOSTON'S NPR® NEWS STATION

Tweeter Speaker

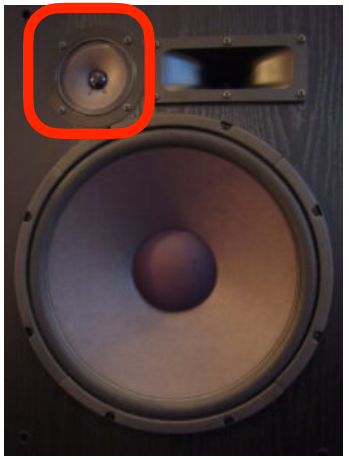


Photo credits: nidcd.nih.gov, audioengine.com

Resonance

MBTA Boylston Station Wheel Squeal

14K views 8y ago ...more

WBUR 27.9K Subscribe

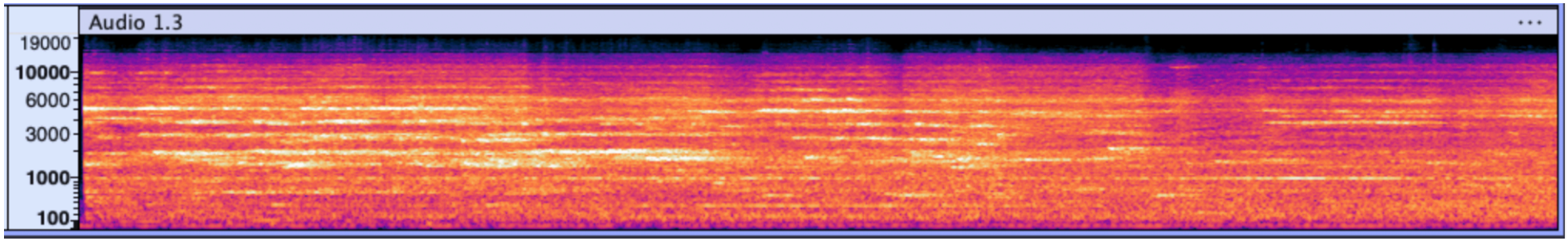


Photo credits: Wikipedia,

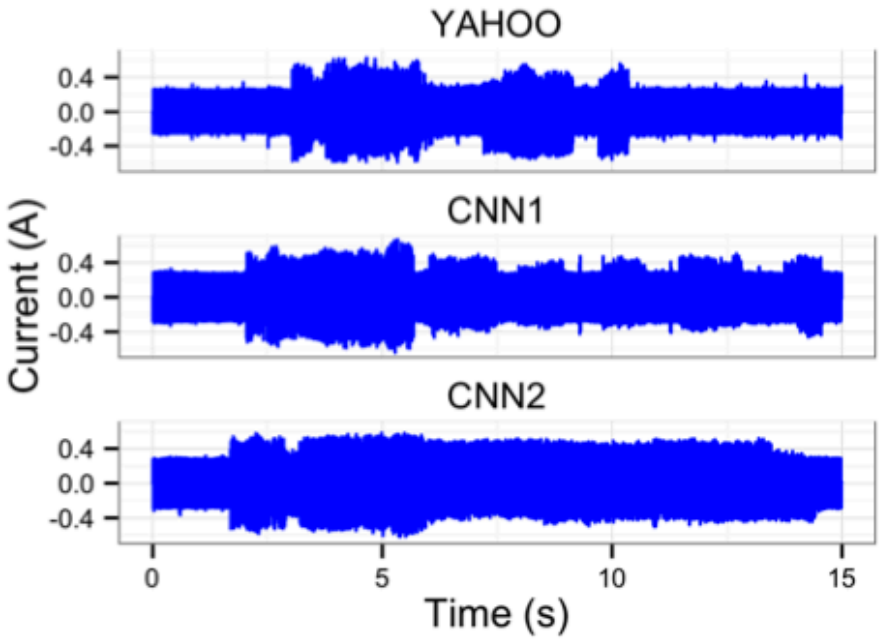
Essay Ideation

- 15 minutes to brainstorm easy #1

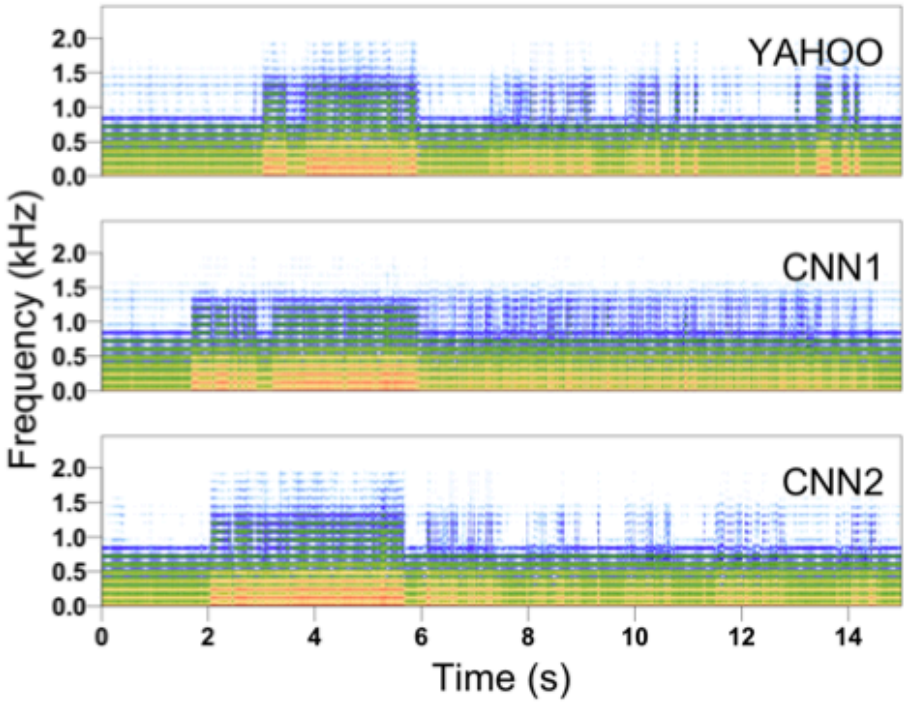
Shannon Nyquist Sampling Theory

- Why must sample at twice the frequency?
- Need two volunteers

Example: Reactive Power

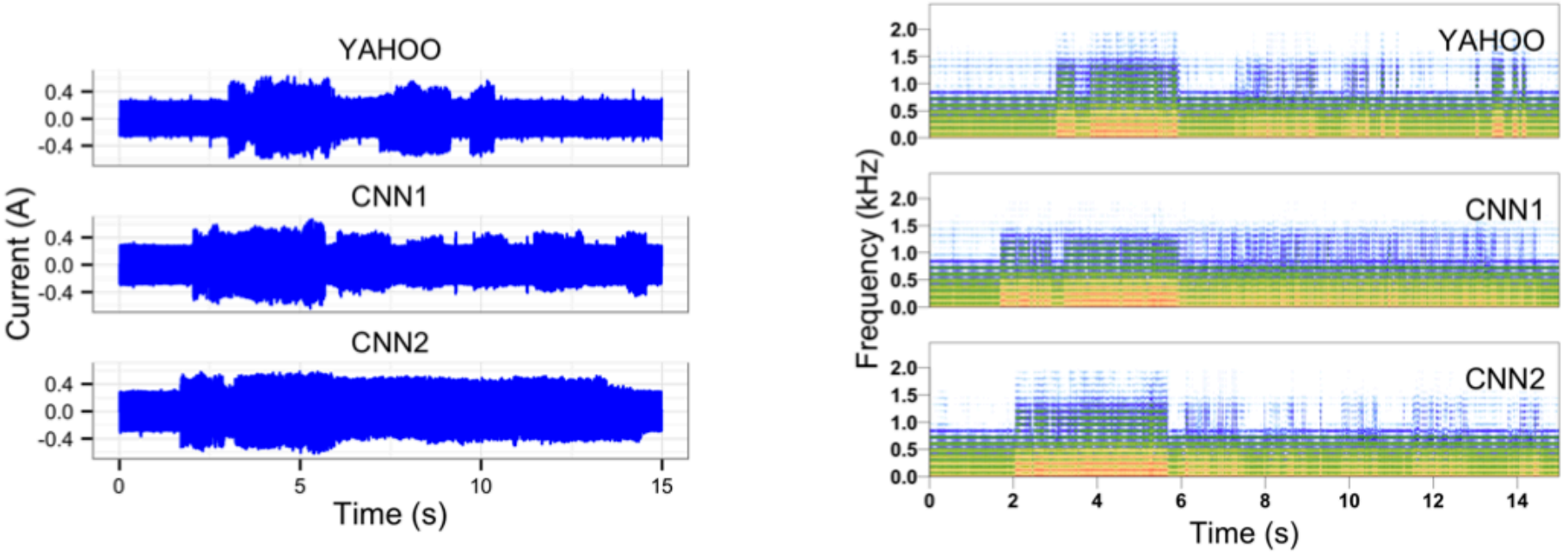


(a) Time-domain plots



(b) Spectrogram plots

Example: Reactive Power



(a) Time-domain plots

(b) Spectrogram plots

Fig. 1: Time- and frequency-domain plots of several power traces as a MacBook loads two different pages. In the frequency domain, brighter colors represent more energy at a given frequency. Despite the lack of obviously characteristic information in the time domain, the classifier correctly identifies all of the above traces.

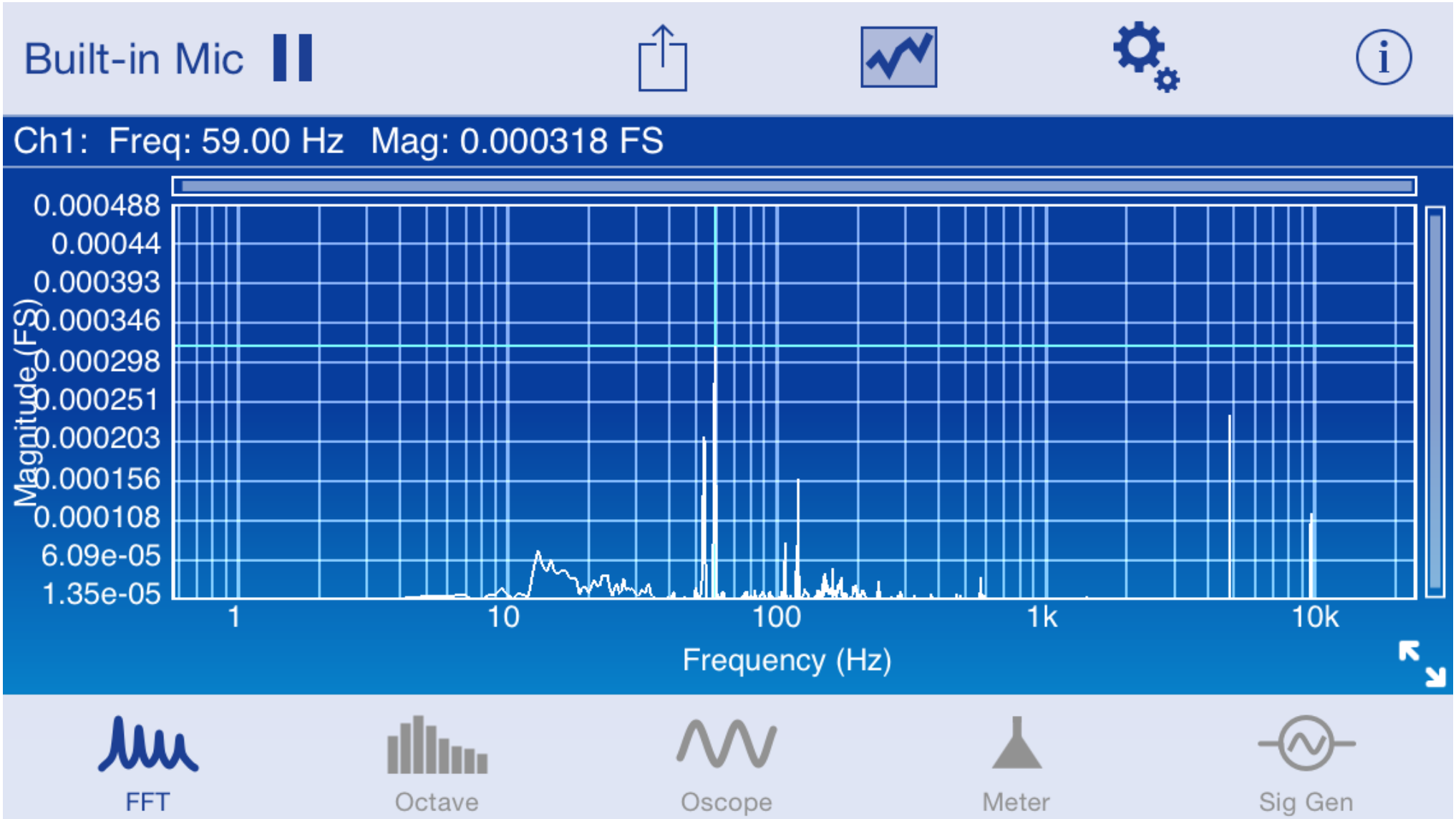
Current Events: Identifying Webpages by Tapping the Electrical Outlet

Shane S. Clark[1], Hossen Mustafa[2], Benjamin Ransford[3],
Jacob Sorber[4], Kevin Fu[5], and Wenyuan Xu[**2,6]

[1]University of Massachusetts Amherst [2]University of South Carolina
[3]University of Washington [4]Clemson University [5]University of Michigan
[6]Zhejiang University

ESORICS 2013

Example: Sound



Turned out to be the HVAC system. The AC conduit line had been mechanically coupled to a ceiling joist near an incandescent lightbulb. The sounds came from the lightbulb. Solved by opening the ceiling, duct taping the AC conduit line. The motor ran at 60hz presumably, causing 60hz sound. Not sure where the 5khz came from. The 10khz is probably the 2nd harmonic.

Signal-to-Noise

- SNR

  ✴= signal to noise ratio

  ✴= survival of signal in noise
- Could you inject whistling signal from 10 miles away? In theory, yes; in practice, no.
- Reality check: path loss makes attacks harder

Homework and Next

- Homework
  - ✓ Prelab #1: Already past due
  - ➡ Lab #1: Due Monday, Sep 22
  - ➡ Essay #1: Assigned
- Next
  - Thursday: Transductions Attacks and Electromagnetic Injection
  - Read: FuXu, “Risks of Trusting the Physics of Sensors,” CACM, 61(2), February 2018.