CIS 700/002: Special Topics: Acoustic Injection Attacks on MEMS Accelerometers

Thejas Kesari
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

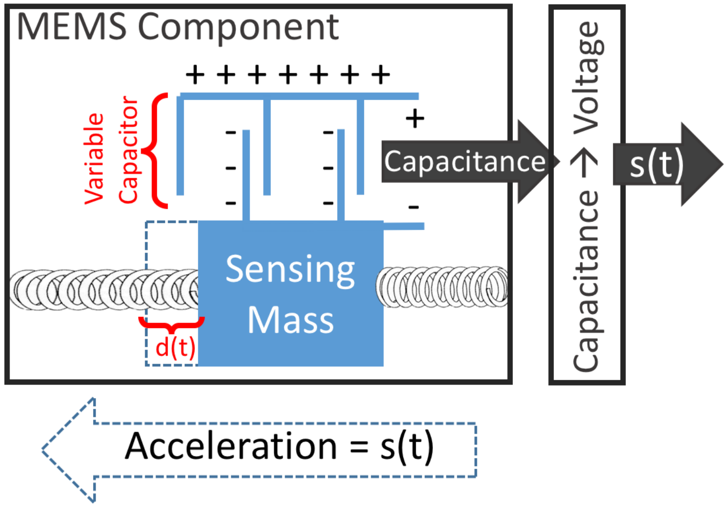
24 March 2017

The Idea

- Compromise digital integrity of Capacitive MEMS Accelerometer
- Deliver chosen digital values

MEMS Accelerometer

- Sensing mass connected to springs that is displaced
- When accelerated, the displacement of mass creates an electrical signal due to change in capacitance
- Measured acceleration s(t) relates to the displacement of mass d(t)
- $F = m\,a$
- $F = -k{\downarrow}s\ \ d$



Prior Art

- Sensors can be tricked by maliciously fabricated physical properties
- An adversary could incapacitate drones equipped with MEMS gyroscopes using intentional sound noise
- Resonant frequency has been identified as a problem that causes the performance degradation of MEMS gyroscopes
- Acoustic interference can hence cause DoS attacks

-Yunmok Son, et. al., *Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors*, 24th USENIX, August 2015

MEMS Accelerometer

- If the acoustic frequency tuned correctly, it can vibrate the sensing mass altering sensor output
- The sensor output can also be altered in a predictable way
- Two problematic components in the signal conditioning path:
  - Insecure LPF
  - Insecure amplifier

MEMS Accelerometer

- Insecure LPF and Insecure Amplifier explain the root cause of DoS attacks
- Also, enabled design two more classes of attacks:
    - Output biasing
    - Output control

More Prior Art

- Defending against malicious acoustic interference by applying acoustic dampening materials (elastomers, microfibrous metallic cloth, felt, etc) **
- Provide physical isolation from the noise ***
- Make the actuator and sensor operate in tandem, provide a challenge-response mechanism ^*

**P. Soobramaney, *Mitigation of the Effects of High Levels of High-Frequency Noise on MEMS Gyroscopes*, Ph.D. dissertation, Auburn University, 2013

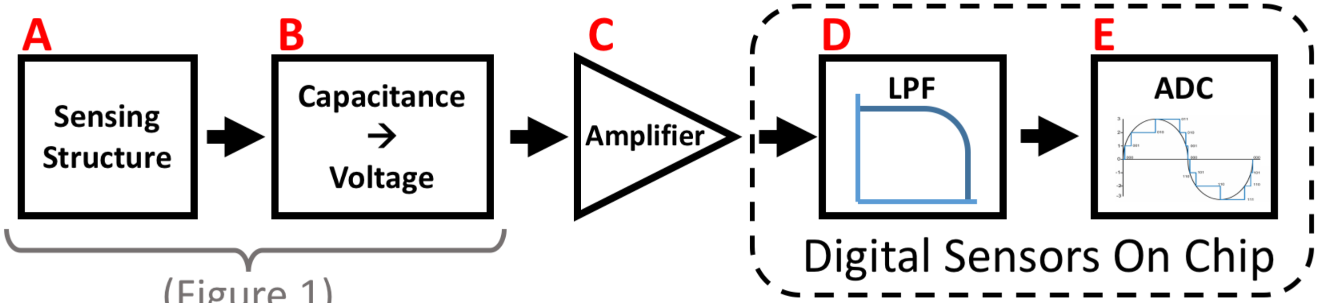
***Yunmok Son, et. al., *Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors*, 24th USENIX, August 2015

^*Y. Shoukry, et. al, *Pycra: Physical challenge-response authentication for active sensors under spoofing attacks*, in Proc. ACM CCS, 2015

More Prior Art

- Impractical – increases packaging size
- Not always applicable – sensor must operate with an actuator in a closed loop system
- Insufficient – not an exhaustive method and cannot filter out all interference

Architecture



(Figure 1)

- Additional processing is required for the electrical acceleration signals to interface with microprocessors
- Change in capacitance is converted to a voltage, amplified, filtered, and digitized
- Without stage D, aliasing can occur, enabling output biasing attacks
- Signal clipping at C can introduce a DC component into the acceleration signal, enabling output control attacks

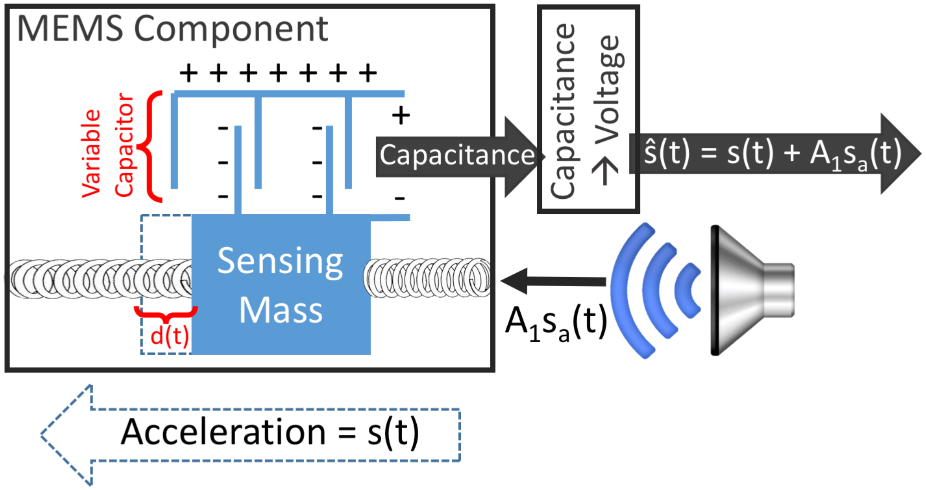
Threat Model

- Attackers neither access the sensor readings directly nor physically touch the sensor
- Do not assume “lunchtime attack”, but assume he is able to reverse engineer a sample device to extract the exact accelerometer model and profile its behaviour under different amplitudes and frequencies
- Attacker is able to induce sound in the vicinity of the victim device in the audible frequency range

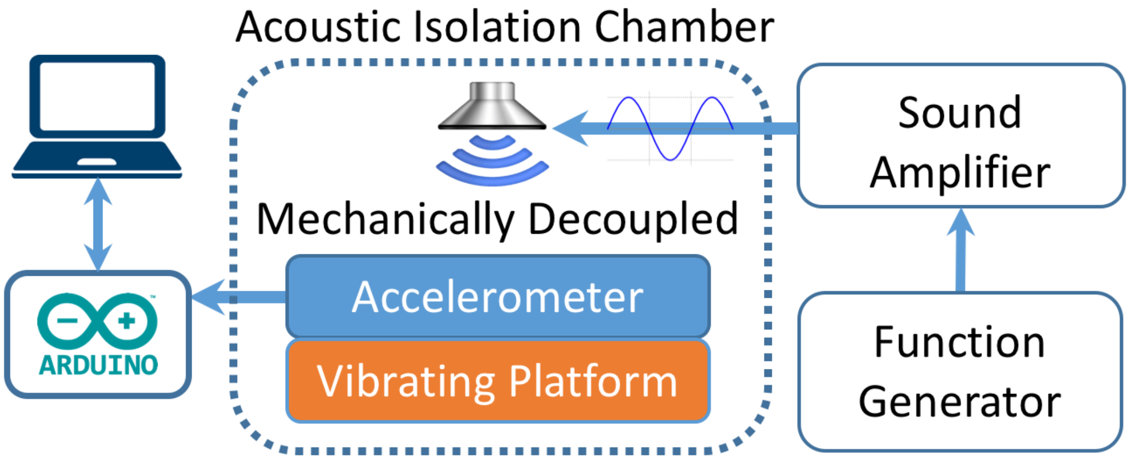
Attack Modeling

- Forces from acoustic waves can also displace the mass
- True acceleration: $s(t)$
- Acoustic: $s_a(t)$

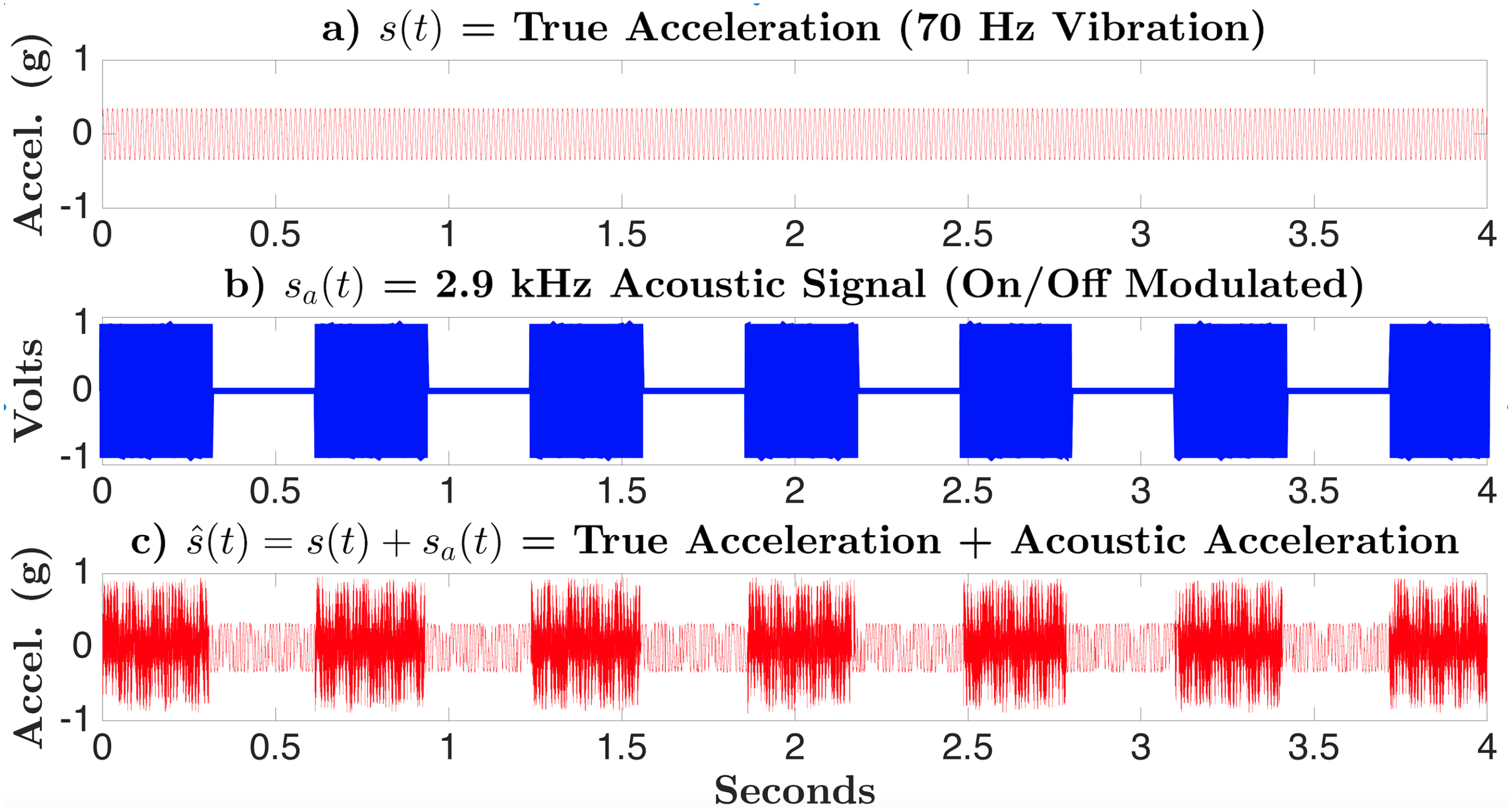
For acoustic frequency F_a, with amplitude A_0 and phase $\emptyset$, the measured acceleration becomes



Attack Modeling



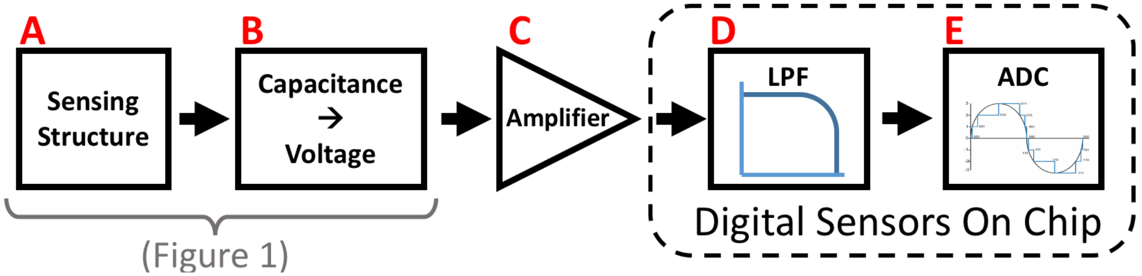
Attack Modeling



Maximize the impact

- $s (t)=s(t)+A_1 s_a (t)$
- Maximize the attenuation co-efficient A_1
- Resonance!
- $A_1 =1$ at resonant frequencies

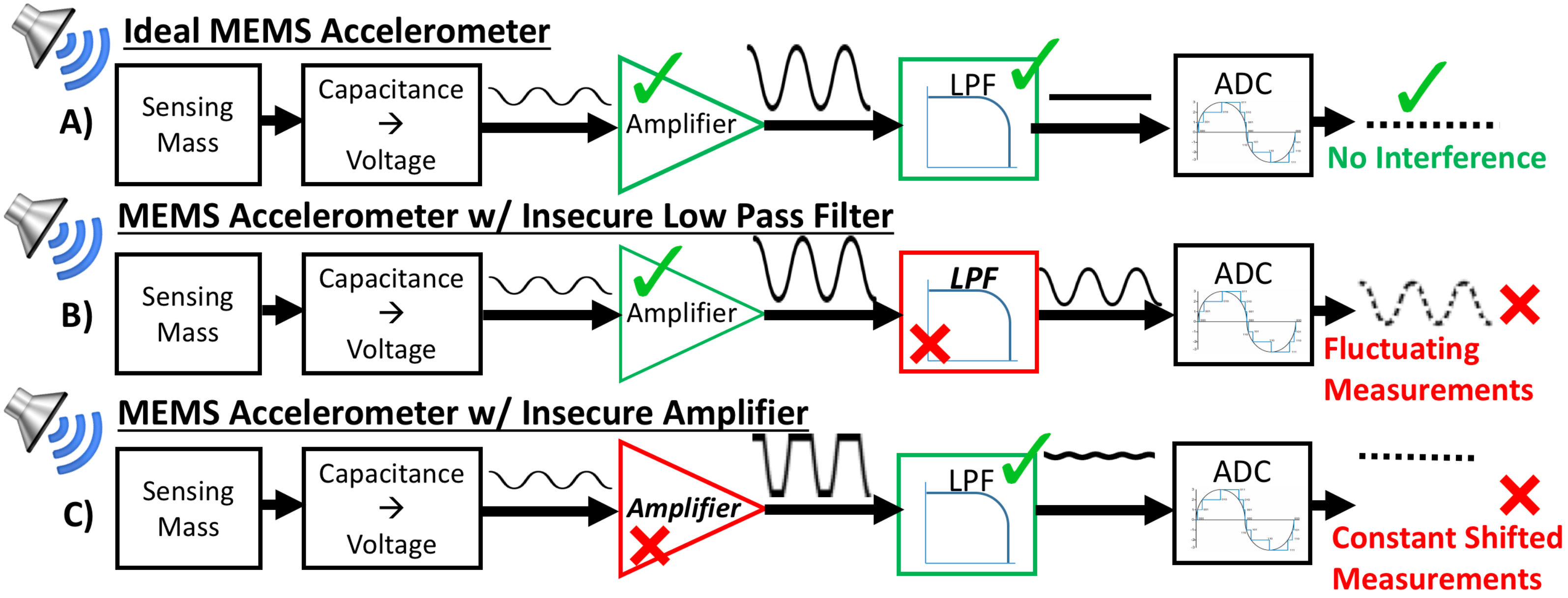
Hardware Deficiencies



A Sensing Structure → B Capacitance → Voltage → C Amplifier → D LPF → E ADC

Digital Sensors On Chip

(Figure 1)



Ideal MEMS Accelerometer

A) Sensing Mass → Capacitance → Voltage → Amplifier ✓ → LPF ✓ → ADC → ✓

No Interference

MEMS Accelerometer w/ Insecure Low Pass Filter

B) Sensing Mass → Capacitance → Voltage → Amplifier ✓ → *LPF* ✗ → ADC → ✗

Fluctuating Measurements

MEMS Accelerometer w/ Insecure Amplifier

C) Sensing Mass → Capacitance → Voltage → *Amplifier* ✗ → LPF ✓ → ADC → ✗

Constant Shifted Measurements

Hardware Deficiencies

- True measurements: No signal clipping occurs; LPF attenuates high frequency acoustic acceleration signals
- Fluctuating False Measurements: No signal clipping; LPF does not completely attenuate HF acoustic signals (under-sampled by ADC)
- Constant Shifted False Measurements: Signal clipping occurs and introduces a non-zero DC component into the amplified signal. Secure LPF passes the DC signals and block HF.

Finding Resonant Frequency

- A sensor at rest should measure constant acceleration of 0 g along the X and Y axes and 1 g along the Z axis
- If at a particular frequency, output measurements are *fluctuating* or *constantly shifted*, then that is the resonant frequency
- By sweeping an acoustic frequency range and acquiring several acceleration measurements at each frequency, both scenarios can be observed

Finding Resonant Frequency: Results

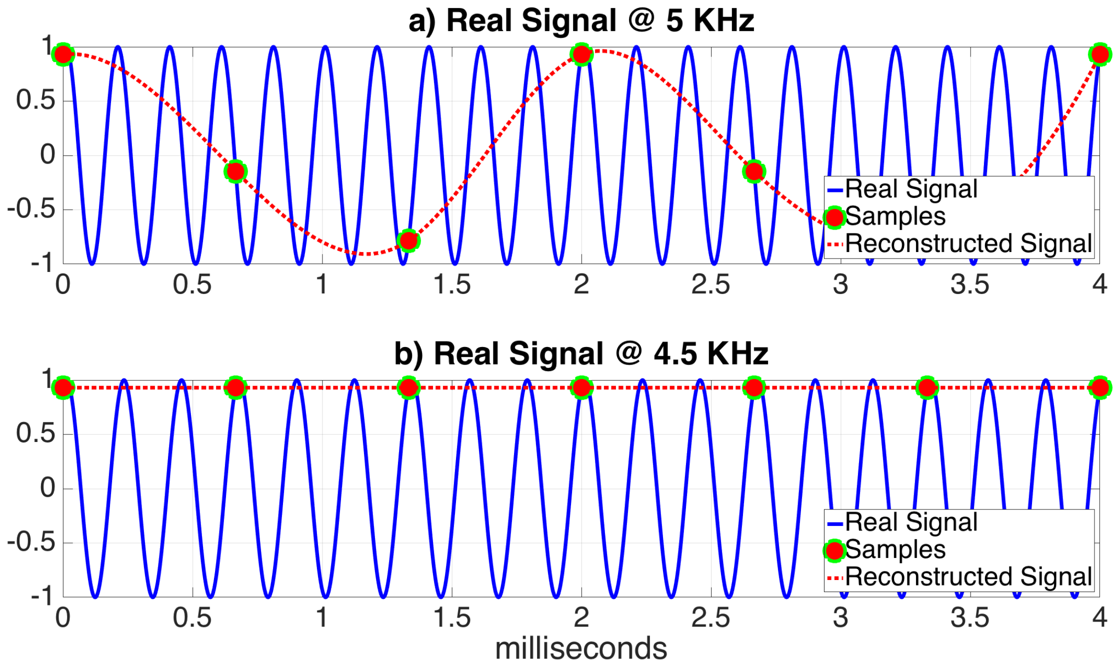
- Both instances of the same sensor behaved identically
- Resonant frequencies can fall in a range, not a single value
- Some sensors have multiple resonant frequencies
- Some sensors have resonant frequencies which result in all combinations of *constant shifted* or *fluctuating*
- Most sensors that were not affected by acoustic interference are physically larger than those that were

Output Biasing Attack

- Pertains to accelerometers that experience *fluctuating* false measurements at their resonant frequencies due to insecure LPF
- To perform this attack, step one:
  - Stabilize fluctuating false measurements to constant ones by shifting the acoustic resonant frequency to induce a DC alias at the ADC. How?
  - How? Signal aliasing. Recall: Nyquist sampling theorem

Output Biasing Attack

- Signal aliasing: Misinterpretation of an analog signal caused by digitizing it with inadequate sampling rate



a) Real Signal @ 5 KHz

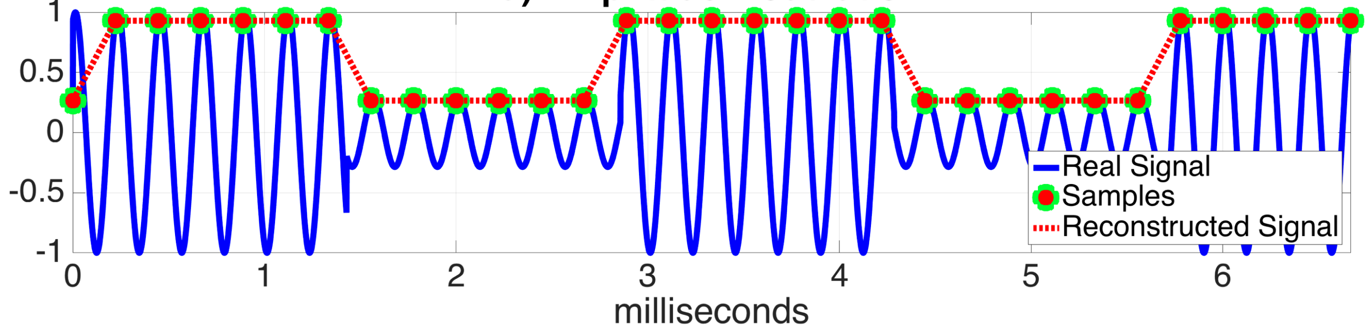
b) Real Signal @ 4.5 KHz

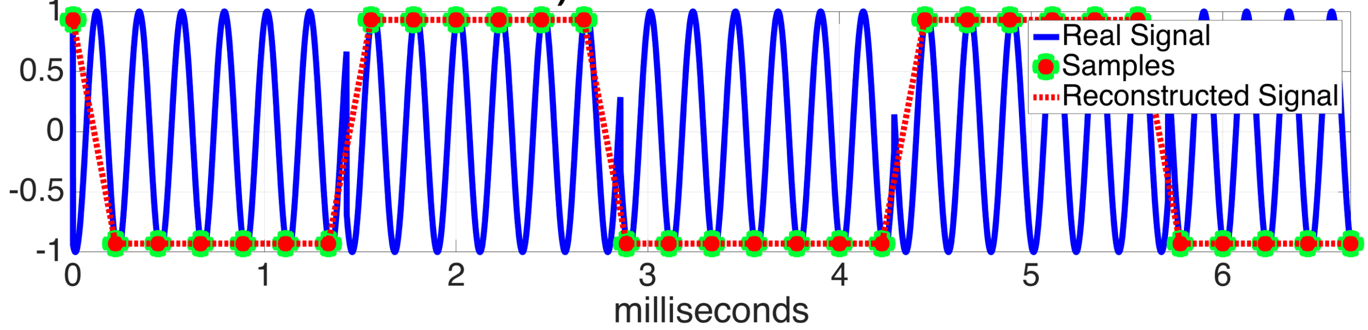
Output Biasing Attack

- To perform this attack, step two:
  - Reshape the desired output signal by modulating it on top of the acoustic resonant frequency.
  - How? AM and PM
- Signal Modulation is used to transmit arbitrary information signals over another carrier signal

Output Biasing Attack

- Sinusoidal Carrier $f_c(t) = A\sin(2\pi f t + \phi)$


a) Amplitude Modulation

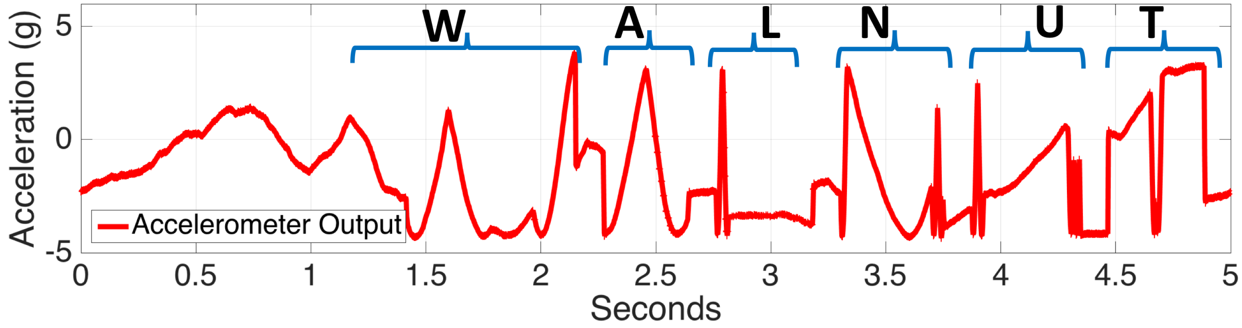

b) Phase Modulation

Output Biasing Attack

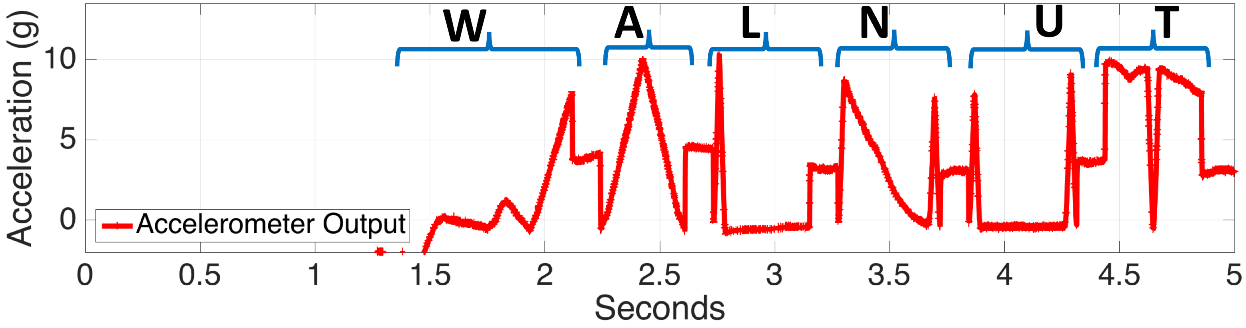
- F_{samp} is fixed
- Resonant frequencies might be a range: frequency deviation f_{e}
- Acoustic frequency: $F_{a}=F_{res}+f_{e}$ (find f_{e} such that the sum is still within resonance)
- Then choose AM or PM to further shape the output signal

Output Biasing Attack

a) Output Biasing on ADXL350 (Inaccurate ADC)



b) Output Biasing on ADXL345 (Inaccurate ADC)

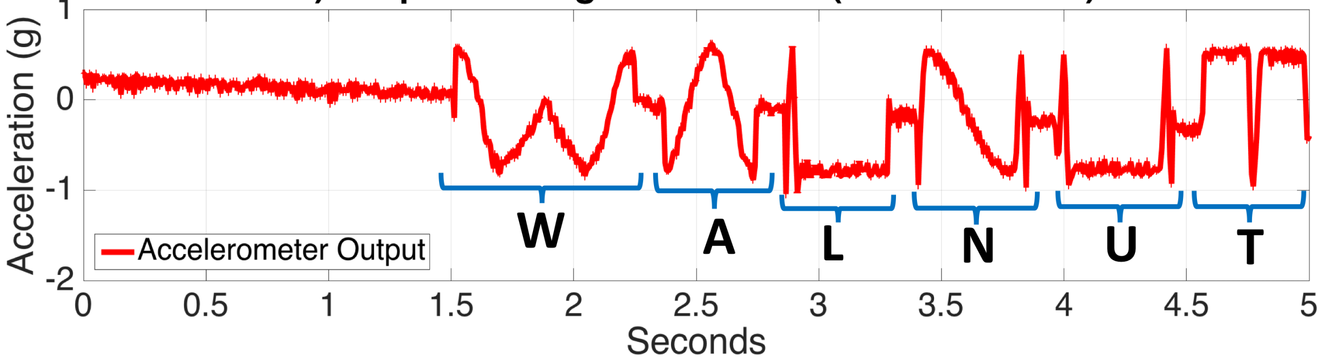


Output Control Attack

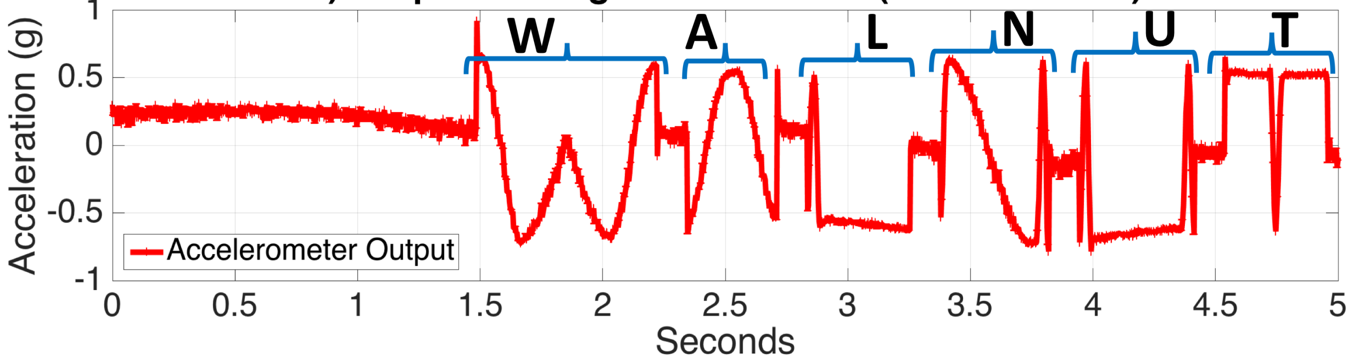
- Applicable to accelerometers that exhibit constant shifted false measurements at their resonant frequencies due to insecure amplifiers
- To perform this attack: reshape the output signal by modulating it over resonant frequency
- Achieving fine grain control requires AM

Output Control Attack

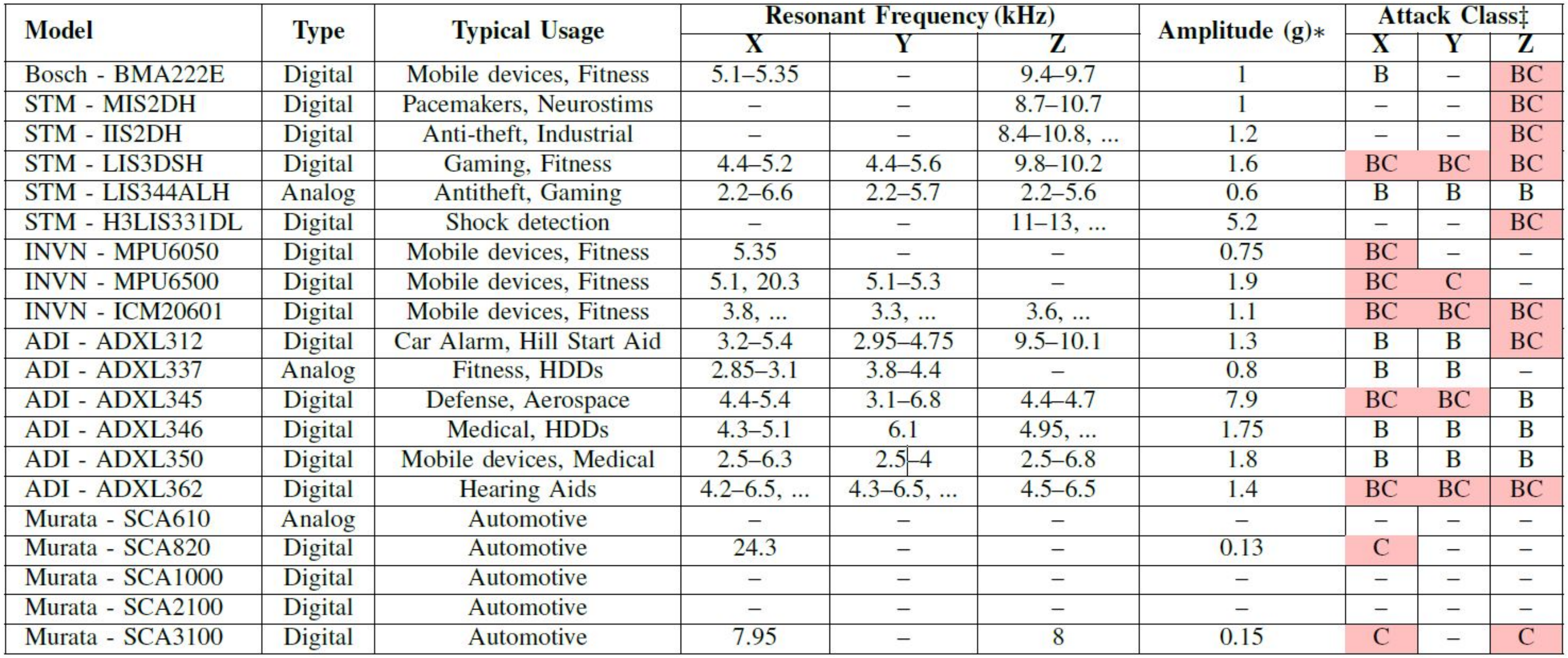
a) Output Biasing on ADXL337 (Accurate ADC)



b) Output Biasing on LIS344ALH (Accurate ADC)



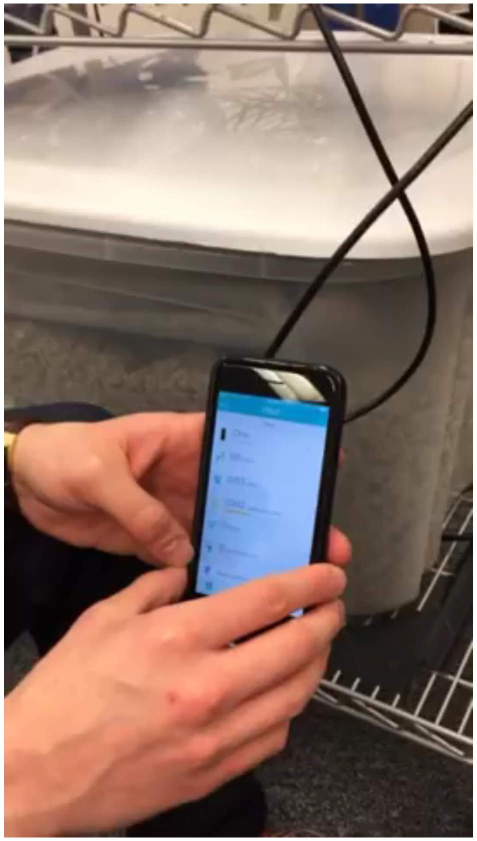
Controlling Accelerometer Output



Model	Type	Typical Usage	Resonant Frequency (kHz)			Amplitude (g)∗	Attack Class‡		
			X	Y	Z		X	Y	Z
Bosch - BMA222E	Digital	Mobile devices, Fitness	5.1–5.35	–	9.4–9.7	1	B	–	BC
STM - MIS2DH	Digital	Pacemakers, Neurostims	–	–	8.7–10.7	1	–	–	BC
STM - IIS2DH	Digital	Anti-theft, Industrial	–	–	8.4–10.8, ...	1.2	–	–	BC
STM - LIS3DSH	Digital	Gaming, Fitness	4.4–5.2	4.4–5.6	9.8–10.2	1.6	BC	BC	BC
STM - LIS344ALH	Analog	Antitheft, Gaming	2.2–6.6	2.2–5.7	2.2–5.6	0.6	B	B	B
STM - H3LIS331DL	Digital	Shock detection	–	–	11–13, ...	5.2	–	–	BC
INVN - MPU6050	Digital	Mobile devices, Fitness	5.35	–	–	0.75	BC	–	–
INVN - MPU6500	Digital	Mobile devices, Fitness	5.1, 20.3	5.1–5.3	–	1.9	BC	C	–
INVN - ICM20601	Digital	Mobile devices, Fitness	3.8, ...	3.3, ...	3.6, ...	1.1	BC	BC	BC
ADI - ADXL312	Digital	Car Alarm, Hill Start Aid	3.2–5.4	2.95–4.75	9.5–10.1	1.3	B	B	BC
ADI - ADXL337	Analog	Fitness, HDDs	2.85–3.1	3.8–4.4	–	0.8	B	B	–
ADI - ADXL345	Digital	Defense, Aerospace	4.4-5.4	3.1–6.8	4.4–4.7	7.9	BC	BC	B
ADI - ADXL346	Digital	Medical, HDDs	4.3–5.1	6.1	4.95, ...	1.75	B	B	B
ADI - ADXL350	Digital	Mobile devices, Medical	2.5–6.3	2.5–4	2.5–6.8	1.8	B	B	B
ADI - ADXL362	Digital	Hearing Aids	4.2–6.5, ...	4.3–6.5, ...	4.5–6.5	1.4	BC	BC	BC
Murata - SCA610	Analog	Automotive	–	–	–	–	–	–	–
Murata - SCA820	Digital	Automotive	24.3	–	–	0.13	C	–	–
Murata - SCA1000	Digital	Automotive	–	–	–	–	–	–	–
Murata - SCA2100	Digital	Automotive	–	–	–	–	–	–	–
Murata - SCA3100	Digital	Automotive	7.95	–	8	0.15	C	–	C

Under resonant acoustic interference, an output biasing attack **(B)** class indicates a sensor's falsified measurements fluctuate (insecure LPF) while an output control attack **(C)** class indicates constant falsified measurements are observed (insecure amplifier)

Attacking Embedded Devices: Fitbit



https://www.youtube.com/watch?v=aedOf3cZnEI

Attacking Embedded Devices: Galaxy S5

https://www.youtube.com/watch?v=C8aZ5nBmKH0

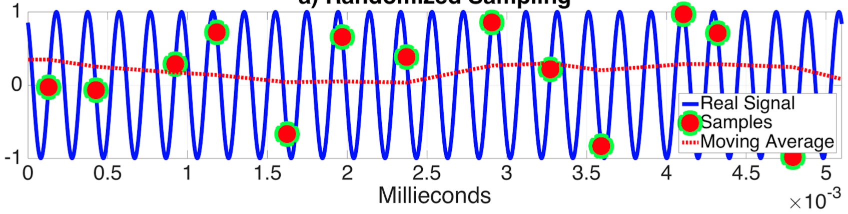
Defence: Hardware Design

- Secure LPF: A properly designed LPF should have a cut-off frequency of less than half of the ADC sampling rate
- Secure Amplifier: Amplifier that can accept large amplitude inputs. Pre-filter acoustic resonant frequencies prior to amplification
- Use of acoustic dampening materials

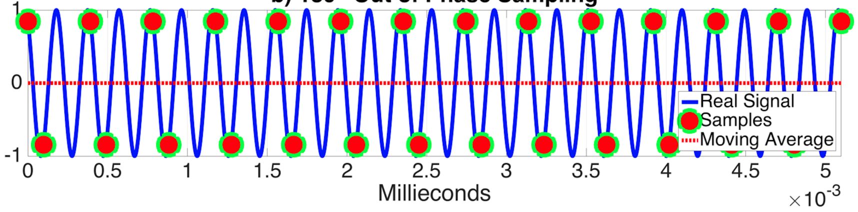
Defence: Software Design

- Randomized sampling: Instead of setting ADC sampling rate fixed, sample at random intervals – prevents attacker from inducing a DC alias
- 180^0 Out-of-Phase Sampling: Attenuates acceleration signals with frequencies around the resonant frequency

a) Randomized Sampling



b) 180^o Out of Phase Sampling



References

- T. Trippel, et. al., “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks”, 2017
- P. Soobramaney, “Mitigation of the Effects of High Levels of High-Frequency Noise on MEMS Gyroscopes”, 2013
- Yunmok Son, et. al., “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors”, 2015
- Y. Shoukry, et. al., “Pycra: Physical challenge-response authentication for active sensors under spoofing attacks”, 2015