
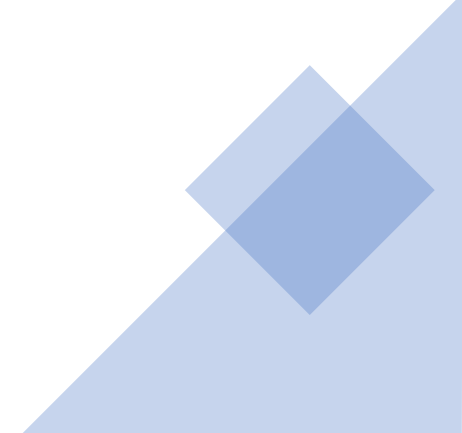


# Resonant Acoustic Injection Attacks

Raul Delioth



*"Great! O.K., this time I want you to sound taller,  
and let me hear a little more hair."*

- 
- 
- Resonant Acoustic Injection
  - Phreaking
  - MEMS Accelerometers
  - Possibilities and Questions

# Resonant Acoustic Injection

- Acoustic Injection: [The Lyre Bird](#)
- [Acoustic Resonance](#): “is a phenomenon in which an acoustic system amplifies sound waves whose frequency matches one of its own natural frequencies of vibration. The term "acoustic resonance" is sometimes used to narrow mechanical resonance to the frequency range of human hearing, but since acoustics is defined in general terms concerning vibrational waves in matter, acoustic resonance can occur at frequencies outside the range of human hearing.” (Wikipedia)
- [Mechanical Resonance: breaking glass with sound vis resonance.](#)



# Phreaking (phone + freak)

- [1950s,60s,70s](#). Captain Crunch (a.k.a. [John Draper](#)), Steve Wozniak, disconnecting calls, free calls, international calls, subculture, social engineering.
- [Blue boxes](#), [black boxes](#), [red boxes](#).
- The predecessor of computer hacking.



Blue box designed and built by [Steve Wozniak](#) and sold by [Steve Jobs](#) before they founded [Apple](#). Displayed at the [Powerhouse Museum](#), from the collection of the [Computer History Museum](#)<sup>[1]</sup>

# Microelectromechanical Systems (MEMS) Accelerometers and Gyroscopes

- [Piezoelectric accelerometers vs MEMS and Gyroscopes.](#)
- MEMS used in rockets, airplanes, ships, cars, phones, smart-watches, military, VR headsets, drones, industrial and consumer robotics, etc.

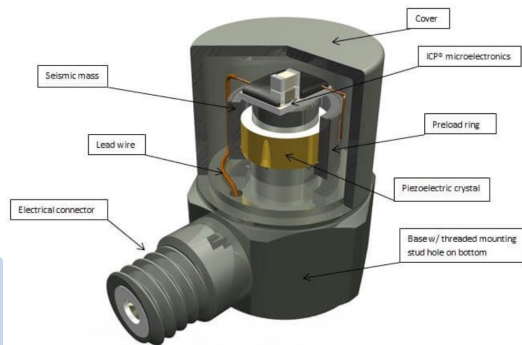
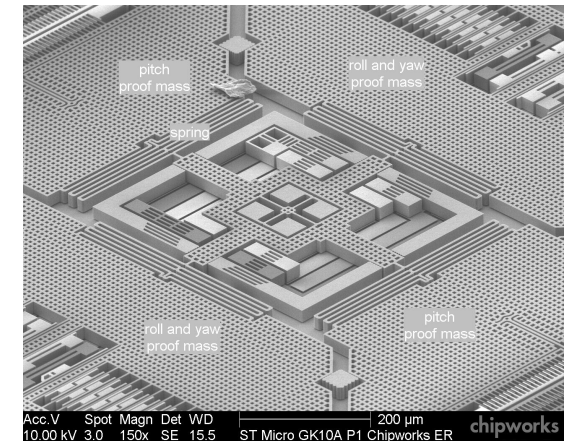
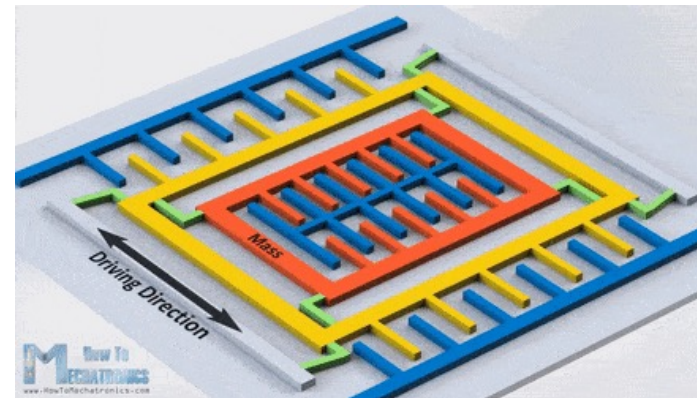
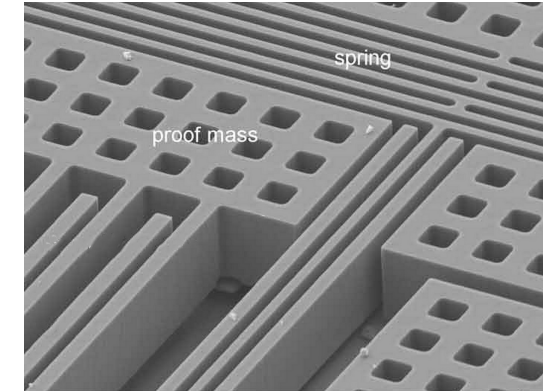
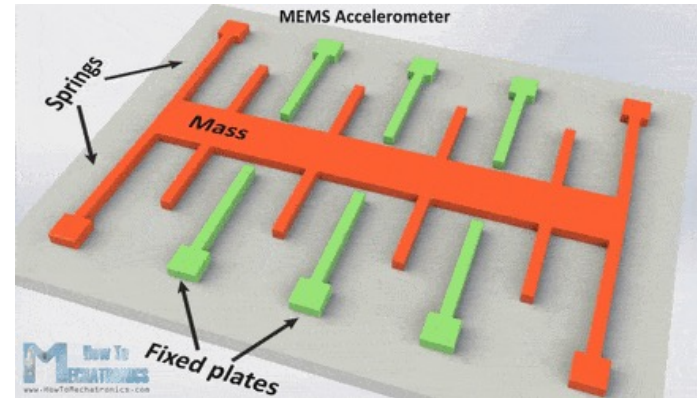
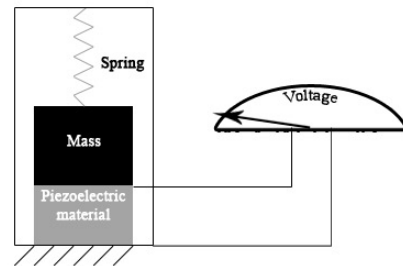


Figure 1: Typical ICP® Accelerometer



# WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks

- [T. Trippel, O. Weisse, W. Xu, P. Honeyman and K. Fu, "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks," 2017 IEEE European Symposium on Security and Privacy \(EuroS&P\), 2017, pp. 3-18, doi: 10.1109/EuroSP.2017.4](https://doi.org/10.1109/EuroSP.2017.4)

“Cyber-physical systems depend on sensors to make automated decisions. Resonant acoustic injection attacks are already known to cause malfunctions by disabling MEMS-based gyroscopes. However, an open question remains on how to move beyond denial of service attacks to achieve full adversarial control of sensor outputs. Our work investigates how analog acoustic injection attacks can damage the digital integrity of a popular type of sensor: the capacitive MEMS accelerometer. Spoofing such sensors with intentional acoustic interference enables an out-of-spec pathway for attackers to deliver chosen digital values to microprocessors and embedded systems that blindly trust the unvalidated integrity of sensor outputs.”

2017 IEEE European Symposium on Security and Privacy

## WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks

Timothy Trippel, Ofir Weisse, Wenyuan Xu\*, Peter Honeyman, Kevin Fu  
*Computer Science and Engineering, University of Michigan*  
*\*Computer Science and Engineering, University of South Carolina*  
<https://spqr.eecs.umich.edu/walnut/>

**Abstract**—Cyber-physical systems depend on sensors to make automated decisions. Resonant acoustic injection attacks are already known to cause malfunctions by disabling MEMS-based gyroscopes. However, an open question remains on how to move beyond denial of service attacks to achieve full adversarial control of sensor outputs. Our work investigates how analog acoustic injection attacks can damage the digital *integrity* of a popular type of sensor: the capacitive MEMS accelerometer. Spoofing such sensors with intentional acoustic interference enables an out-of-spec pathway for attackers to deliver chosen digital values to microprocessors and embedded systems that

### 1. Introduction

With the proliferation of motion-driven applications and Microelectromechanical systems (MEMS) technologies, MEMS accelerometers have been widely used in cyber-physical systems, such as implantable medical devices, automobiles, avionics, and even critical industrial systems [1], [2], [3], [4], [5], [6]. These systems deploy layers of software that abstract away hardware details to collect and analyze data provided by sensors, and then autonomously react to sensor data in real time. The software assumes that

# WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks

Figure 1. **Functional Diagram of Capacitive MEMS Accelerometer** based on [10], [11]. When accelerated, the displacement of the mass creates an electrical signal due to a change in capacitance. The measured acceleration,  $s(t)$ , relates to the displacement of the mass,  $d(t)$ , according to Newton's second law of motion,  $F = m \cdot a$ , and Hooke's law,  $F = -k_s \cdot d$ .

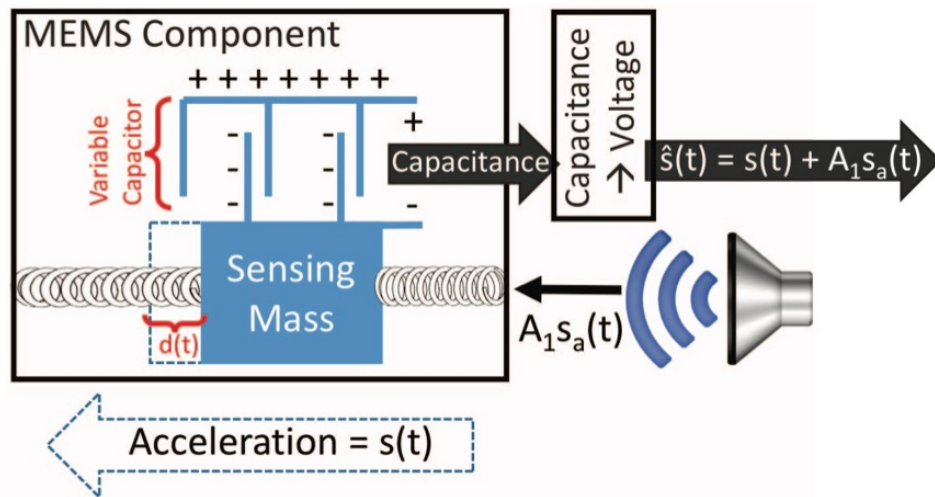


Figure 3. **Acoustic Interference Disturbs Acceleration Measurements.** True acceleration and acoustic interference can both displace the mass, creating electrical acceleration signals. The measured acceleration,  $\hat{s}(t)$ , is a linear combination of true acceleration,  $s(t)$ , and acoustic acceleration,  $s_a(t)$ .

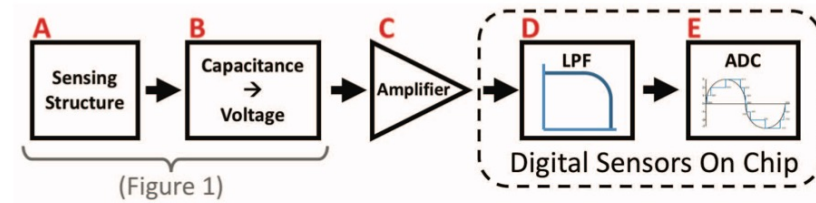


Figure 2. **Typical architecture of the signal conditioning path in a MEMS accelerometer** based on [10]. The change in capacitance measured by a sensing mass (Fig. 1) is converted to a voltage, amplified, filtered, and digitized. Without stage D aliasing can occur, enabling *output biasing* attacks. Signal clipping at C can introduce a DC component into the acceleration signal, enabling *output control* attacks.

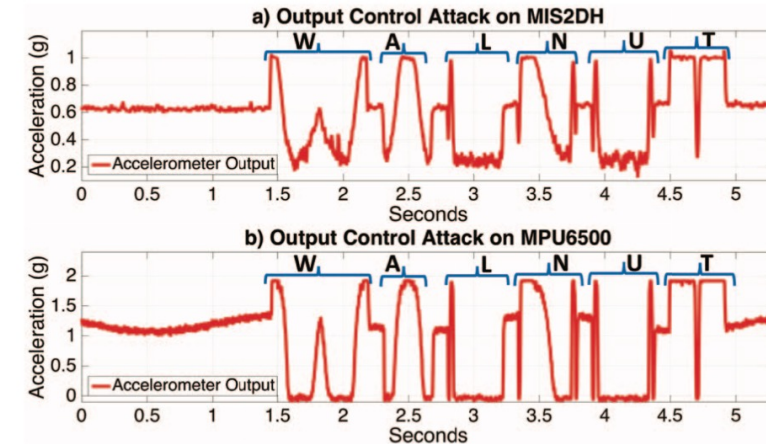


Figure 12. **Spelling WALNUT: Output Control Attack.** We demonstrate the output control attack achieving full indefinite control over the X-axis acceleration signals of the a) MIS2DSH and b) MPU6500 accelerometers, spoofing the sensor to spell out “WALNUT”. Each accelerometer was positioned with the Z axis aligned with gravity, so the X axis output should have measured 0g. This attack leverages a security-flaw in the amplifier of specific accelerometers. The attacker does not need to know anything about the sampling regime of the ADC, hence the WALNUT signal is the least distorted compared with Figs. 10 and 11.

# WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks

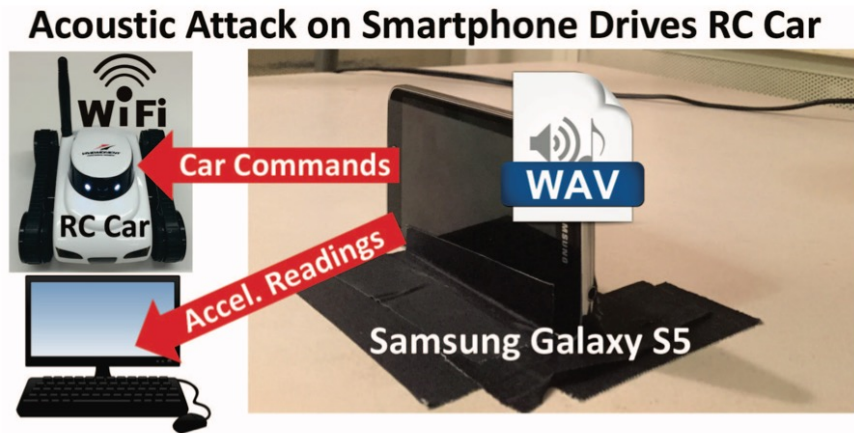


Figure 13. **Smartphone Attacking its own Accelerometer to Control an RC Car.** An Android phone runs an application that controls an RC car based on the phone's orientation, measured by its internal MEMS accelerometer. Simultaneously, a malicious audio file is playing over the phone's speaker, mounting an output control attack on the phone's accelerometer. The RC car is essentially piloted by the audio file.

## 7.3. Free Fitbit Rewards

Several companies, including Walgreens and Higi, incentivize people to exercise by offering rewards programs that tether to their personal fitness tracking wristbands and monitor their daily physical activity. These fitness tracking wristbands use accelerometer driven pedometers [1] to count the number of steps the user takes over the course of a day. Rather than exploiting software vulnerabilities to spoof step counts [22], we demonstrate how one can spoof approximately 3,000 steps an hour on a Fitbit One [23] fitness tracker using acoustic interference and earn free rewards.

We opened a Higi.com account and tethered a Fitbit One device to the account. Using a similar setup as shown in Figure 4, absent the vibrating platform, acoustic interference at the resonant frequency of the Fitbit's accelerometer was played for approximately 40 minutes. No signal aliasing or modulation was needed as simply spoofing fluctuating false measurements was sufficient to register thousands of false steps. We were able to register 2,100 steps in that time and earn 21 rewards points on Higi.com without walking a single step. Due to ethical considerations, we have not claimed any of these rewards and have notified the respective manufacturers about such flaws.

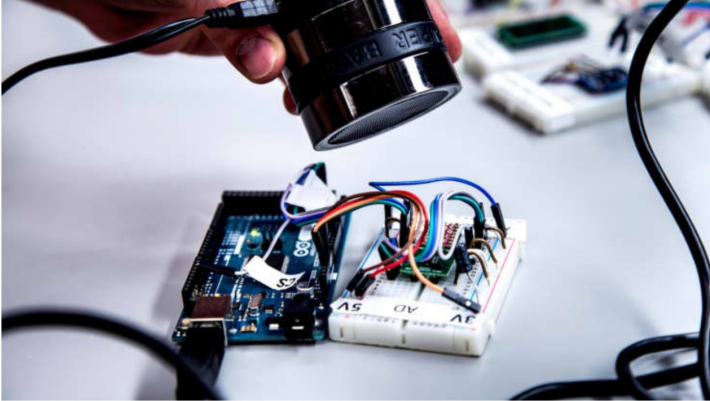


# It's possible to hack a phone with sound waves, researchers show

PUBLISHED TUE, MAR 14 2017-9:58 AM EDT | UPDATED TUE, MAR 14 2017-10:55 AM EDT

The New York Times | John Markoff

SHARE [f](#) [t](#) [in](#) [✉](#)



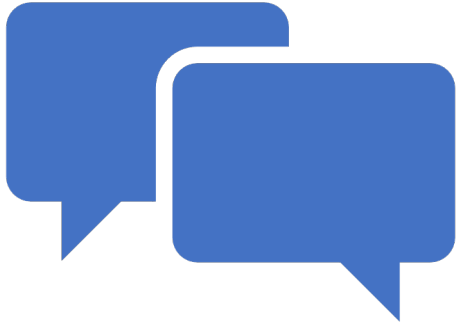
A speaker can make tones that fool a sensor and cause a microprocessor to accept the sensor readings.  
*Joseph Xu | University of Michigan via New York Times*

**TV**  
**American Greed** [WATCH LIVE](#)  
UP NEXT | **Street Signs** 4:00 AM ET [Listen](#)



“It’s like the opera singer who hits the note to break a wine glass, only in our case, we can spell out words” and enter commands rather than just shut down the phone, said Kevin Fu, an author of the paper, who is also an associate professor of electrical engineering and computer science at the University of Michigan and the chief executive of Virta Labs, a company that focuses on cybersecurity in health care. “You can think of it as a musical virus.”

The flaw, which the researchers found in more than half of the 20 commercial brands from five chip makers they tested, illustrates the security challenges that have emerged as robots and other kinds of digital appliances have begun to move around in the world.



# Other Possible Attacks Discussion and Questions

