Eavesdropping Speech with Non-sensing Devices

Tim Holzhey
Technische Universität Berlin
Berlin, Germany
holzhey@campus.tu-berlin.de

ABSTRACT

In recent years, numerous research papers have shown that air pressure waves produced by human speech or other sounds can induce vibrations into an array of non-acoustic sensors (e.g. motions sensors) or into externally measured objects (e.g. laser-based vibrometer) skewing sensor readings in a reversable manner, effectively turning them into undisclosed microphones. This allows for eavesdropping on private speech by maliciously altered devices and therefore posing a real threat to privacy when exploited.

This work will examine and compare different types of vibration-based side channel attacks employed on common IoT and Smart devices to recover speech or infer privacy-sensitive information about the speaker like their identity, political views or gender. We explore the steps taken to take control of the targeted device, gather the necessary data, and perform signal processing and machine learning techniques to extract audible information from the sensor readings. The overview established over the attacks then allows for a comprehensive feasability study for the respective attack methods and complexity required to perform such attacks in a real world scenario. We discuss possible countermeasures to mitigate the risk of such attacks and provide an outlook on future research directions in the field.

CCS CONCEPTS

• Security and privacy → Side-channel analysis and countermeasures; **Embedded systems security**; **• Computer systems organization → Sensors and actuators**.

KEYWORDS

Security, Privacy, Side-channel, Eavesdropping, Speech, Acoustic, Hardware Security, Privacy Leaks

1 INTRODUCTION

While the IoT market is on the rise and still growing exponentially, projected to exceed USD 4 trillion by 2032 [3], this opens up a new attack vector for adversaries to exploit in addition to traditional software vulnerabilities in computers. Latest surveys show that the American households had on average 21 connected devices [2], a relevant part of which are IoT and Smart Home devices. IoT devices are often equipped with a variety of sensors to interface with their physical environment, such as accelerometers, gyroscopes, microphones, and cameras. Many of these sensors can also be found in modern smartphones, which are carried around by most people[1]. Mobile operating systems provide zero-permission access to sensor data from the built-in accelerometer and gyroscope, therefore have been the subject of the majority of research done in this field. The findings from vulnerabilities found in smartphones can be projected onto IoT and Smart devices with similar sensors that do not have a primary function of audio recording i.e. do not have a built-in microphone ("non-sensing"). To execute a vibration-based eavesdropping attack, most of the previous papers took the approuch to exploited MEMS[2] motion sensors (accelerometers, gyroscopes and magnetometers) commonly found in smartphones and many smart devices including smartwatches, fitness trackers, gaming controllers, etc. Some of the more experimental approaches have also shown that other sensors like Lidar scanners in vacuum cleaners, the position error signal of write heads in hard drives or electro-optical sensors directed at ceiling lights can be exploited for similar attacks.

CONTRIBUTION: Altough parts of the available research material in this field is investigating keystroke recovery attacks [9][11][27] or is using sophisticated external setups (e.g. RFID-Tags [13], millimeter-waves [12], WiFi radio [25]), we limit the scope of this paper to **on-device vibration-based speech and general sound recovery attacks**. This includes attacks in theory possible without any modified or additional hardware assuming a compromised device or malicious software. This work aims to provide a comprehensive overview of the current state of research in the field of vibration-based eavesdropping attacks on non-sensing devices. We highlight notable research papers and their findings, compare the different attack methods and achieved results, and discuss the feasibility of such attacks in real-world scenarios.

2 BACKGROUND AND LITERATURE REVIEW

2.1 Vibration-based Eavesdropping Attacks

Sound created by a human speaking or any other sound can be characterized as spatially and temporally propagating changes in air pressure in the audible frequency range (20 Hz - 20 kHz). Similarly to how sound waves induce vibrations into our eardrums to let us perceive sound, they can also couple vibrations into all other objects they encounter, more so into objects that are resonant at the frequency of the sound. In a typical microphone, an oscillating diaphragm is used to convert these vibrations into an electrical signal i.e. a change in voltage by varying the capacitance of a capacitor (condenser microphone) or by inducing a current into a coil (dynamic microphone). Even if unintended, the same phenomenon can be used to turn any other sensing electrical component into a microphone if it has a moving part capable of influencing the electrical properties of the component directly (e.g. MEMS, write head of a hard drive) or observing the movement of another object

[1] Surveys from 2024 suggest that 91 % of Americans own a smartphone [5]

[2] Abbr. Micro-electromechanical systems

(e.g. laser vibrometer, Lidar scanner, camera). As audible information was not intended to be captured by these sensors, an attacker who is able to recover this information from the sensor readings is exploiting a side channel vulnerability.

2.2 MEMS-based Eavesdropping Attacks

Sensors manufactured using micro-electromechanical fabrication techniques (MEMS) incorporate electronics and moving parts on a micrometer-scale chip to measure physical parameters like acceleration (accelerometer), orientation and angular velocity (gyroscope) or the magnetic field (magnetometer). The manufactureing process makes use of lithography and etching semiconductor manufacturing techniques on silicon wafers that allows for the production of small, low-cost sensors with high sensitivity and accuracy. They are widely used in consumer electronics to enable features like screen rotation, step counting, navigation and gaming feedback. On a physical level, MEMS sensors are most commonly realized by a spring-suspended proof mass that changes the capacitance of the circuitry when displaced (variable capacitance MEMS) or by a flexible piezoelectric material that changes its electrical resistance when bent (piezoresistive MEMS). The structures can be repeated and aligned in three orthogonal directions to measure the physical property in the three-dimensional spacial domain.

MEMS Accelerometer: An accelerometer measures the proper acceleration (change in velocity) of an object relative to a local inertial reference frame. In the gravitational field of the earth, the accelerometer's measurement is offset by the upwards acceleration of 1 g (9.81 m/s^2) relative to the free-falling reference frame. The basic mechanical structure of an accelerometer consists of a damped proof mass suspended by springs that is displaced when the sensor is accelerated in the opposite direction of movement. In a typical VC MEMS accelerometer, the proof mass moves between air-gapped fixed electrodes forming a variable capacitor as shown in Figure 1.

MEMS Gyroscope: A gyroscope measures the angular velocity (rate of rotation) of an object relative to a local inertial reference frame. Gyroscopes realized as a MEMS sensor are commonly Vibrating structure gyroscopes (VSG) that measure the Coriolis force acting on a vibrating proof mass when the sensor is rotated. As the vibrating mass tends to continue vibrating in the same plane, the Coriolis force deflects the mass in the direction perpendicular to the rotation axis. The deflection is measured by capacitive sensing or piezoresistive sensing and is proportional to the angular velocity of the rotation as shown in Figure 2.

MEMS Magnetometer: A magnetometer measures the strength and direction of the local magnetic field. MEMS-based magnetometers often use the Lorentz force acting on the current-carrying conductor in the magnetic field to move the mechanical structure. The displacement is then measured by capacitive, piezoresistive or optical sensing and is proportional to the magnetic field strength.

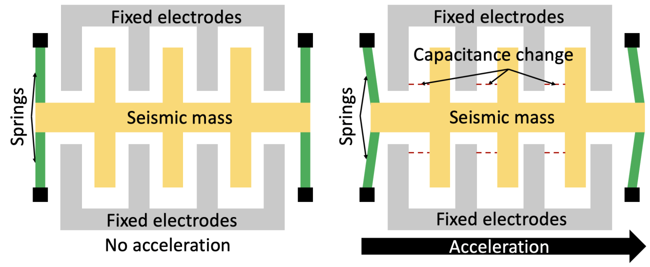

Figure 1: Accelerometer VC MEMS structure, Source: *AccelEve* 2020 [8]

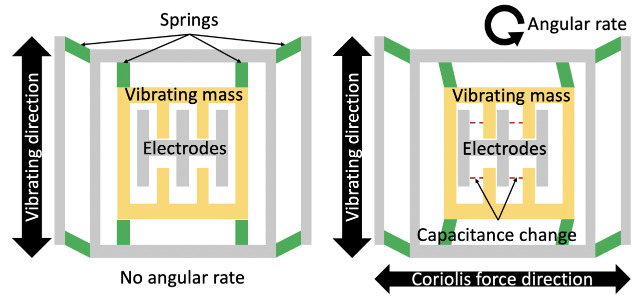

Figure 2: Gyroscope VC MEMS structure, Source: *AccelEve* 2020 [8]

Although MEMS sensors are designed to be best insensitive to acoustic noise which could degrade their signal-to-noise ratio, they are still susceptible to sound waves that induce vibrations in the sensor structure. A MEMS-based eavesdropping attack exploits this vulnerability by recovering the sound-induced vibrations from the sensor readings and reconstructing the original sound.

Early Work: The first and most cited paper able to demonstrate the feasibility of recovering speech from motion sensors was *Gyrophone: Recognizing Speech from Gyroscope Signals* [20] in 2014, a joint efffort by Yan Michalevsky *et al.* from Stanford University and the National Research & Simulation Center (Rafael Advanced Defense Systems Ltd., Isreal). The authors showed that a smartphone's gyroscope can be used to recover speech rendered by a nearby loudspeaker using sensor readings at a well below Nyquist sampling rate of 200 Hz. An Android app was developed to record the gyroscope readings without requiring any special permissions. Later, they used the off-the-shelf *Sphinx* speech recognition system to recognize spoken digits, but also trained custom machine learning models in *Matlab* to identify the speaker and their gender. With a limited dictionary of spoken english digits (0-9), no assumptions about the speaker and a distance of 10 cm between the loudspeaker and the smartphone on a solid table surface, a recognition accuracy of at most 26 % was achieved.

Recent Work: Notably in 2023, Shijia Zhang *et al.* from The Pennsylvania State University leveraged speech eavesdropping attacks using motion sensors in their paper *I Spy You: Eavesdropping Continuous Speech on Smartphones via Motion Sensors* [30] to, for the first time, provide full continuous speech recognition by jointly using accelerometer and gyroscope data. With a large dictionary of 9950 words and a custom ASR (Automatic Speech Recognition) deep learning model, they achieved 53.3 % accuracy in recognizing spoken words on an Android smartphone at a sampling rate of 200-500 Hz.

Most recently in 2024, Qingsong Yao *et al.* from Xidian University, China published the paper *Watch the Rhythm: Breaking Privacy with Accelerometer at the Extremely-Low Sampling Rate of 5Hz* [28] in which they demonstrated that a smartphone's accelerometer can be used for eavesdropping attacks even when limited to a sampling rate of just 5 Hz. This was achieved by extending the machine learning algorithms to not only consider time-frequency features (spectral) but also the temporal dynamics of the signal (pause rhythm and energy intensity rhythm). To benchmark against previous papers, the authors showed that english spoken digits could be recognized with an accuracy of 32.70 % at 5 Hz with an on-device Android app reading accelerometer data.

2.3 Laser-based Eavesdropping Attacks

Laser-based measurement devices (e.g. LiDAR scanners, interferometers, vibrometers) are used in various applications to measure precise distances, velocities and material properties contactlessly in various scientific, industrial and medical applications, but recently also in consumer electronics. Prominently, LiDAR scanners are making their way into our daily lifes as they are used in autonomous vehicles, drones, robotic vacuum cleaners, Apple FaceID or Augumented Reality enabled smartphones.

LiDAR Scanner: LiDAR (Light Detection and Ranging) is a remote sensing and imaging technique that uses a pulsed laser beam to measure the distance to a target object by measuring the time it takes for the light to reflect back to the sensor (Time of Flight). 3D LiDAR scanners can map the environment in all directions by rotating the laser beam in a horizontal plane and measuring the distance at different angles (Figure 3). The cummulative distance measurements can be used to create a point cloud representation of the environment. In order to not interfere with other optical sensors (e.g. camera, human eye), LiDAR's wavelength is mainly located in the near-infrared part of the electromagnetic spectrum (750 nm to 1.5µm).

Laser Doppler Vibrometer: A laser microphone uses a laser beam to detect sound vibrations in a distant object. The minute differences in the distance traveled by the light as it reflects from the vibrating object are detected interferometrically. The Laser Doppler Vibrometer (LDV) implements this principle of laser interferometry by splitting the laser into two beams, one of which is reflected off the vibrating object. The surface will module the phase and frequency of the light due to the Doppler effect. One of the beams is passed through a Bragg cell (acousto-optic modulator) to add a frequency shift and then recombined with the other beam to be directed to a photodetector (Figure 4). The electrical signal produced by the photodetector is equal to the carrier frequency produced by the Bragg cell modulated by the Doppler frequency of the vibrating object and proportional to the velocity of the object.

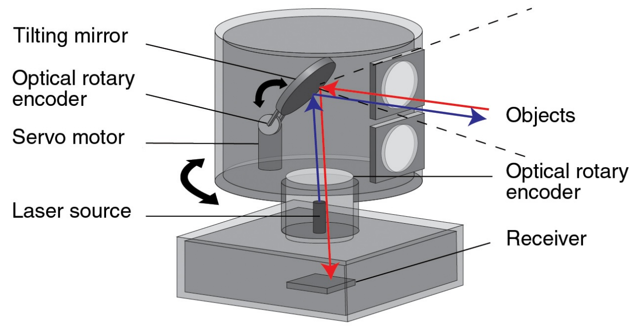

Figure 3: Mechanical spinning LiDAR [1]

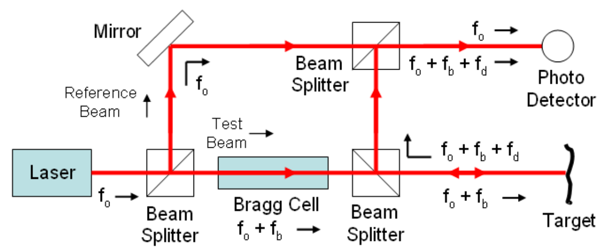

Figure 4: Laser Doppler Vibrometer [4]

Recent Work: In 2020, a group of researchers from the University of Singapore and the University of Maryland sparked the interest of the security research community [14] and news outlets [26] with their paper *Spying with Your Robot Vacuum Cleaner: Eavesdropping via Lidar Sensors* ("Lidarphone") [21]. A method is introduced that repurposes lidar sensors in robot vacuum cleaners to function as laser-based microphones capable of capturing sound signals by detecting subtle vibrations on nearby objects.

2.4 Other Eavesdropping Attacks

3 THREAT MODEL

4 SPEECH RECONSTRUCTION

4.1 Speech Intelligibility

A human speeking in a non-tonal language like English produces a complex waveform that is composed of various frequencies in the audible range. While the fundamental frequency f_0 of the human voice is typically in the range of 100 Hz to 300 Hz (higher for women and children), overtones and consonant articulations can cover most of the audible frequency range of up to 17 kHz (Figure 5). Research has shown that frequencies between 1 kHz and 4 kHz are most important for speech intelligibility [10]. Applying a low-pass filter to the speech signal at 1 kHz and below quickly degrades the intelligibility of the speech to near zero as shown in Figure 6. Since most experimets conducted using motion sensors are limited to a sampling rate of 100-500 Hz, special techniques have to be employed to recover frequencies above the Nyquist frequency $f_N = \frac{1}{2} f_s$ that are essential for speech intelligibility.

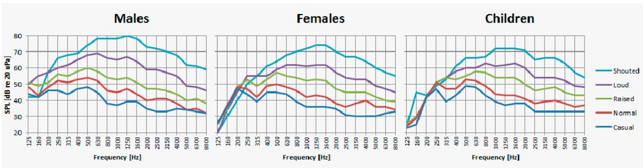

Figure 5: Frequency spectrum of a human voice for Males, Females and Children [10]

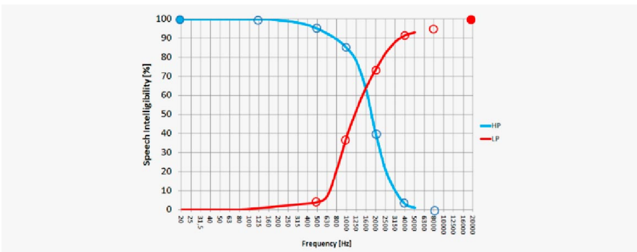

Figure 6: Speech intelligibility with low-pass and high-pass filters applied at various frequencies [10]

4.2 Signal Processing

4.3 Machine Learning

4.4 Automated Speech Recognition

5 FEASIBILITY STUDY

6 COUNTERMEASURES

7 CONCLUSION

REFERENCES

[1] Renishaw plc [n. d.]. *Optical encoders and LiDAR scanning*. Renishaw plc. Retrieved January 07, 2025 from https://www.renishaw.com/en/optical-encoders-and-lidar-scanning--39244

[2] PRNewswire 2023. *Deloitte: The Connected Consumer Paradox - Desire for Fewer Devices vs. More Virtual Experiences and Technology Innovation*. PRNewswire. Retrieved January 07, 2025 from https://www.prnewswire.com/news-releases/deloitte-the-connected-consumer-paradox---desire-for-fewer-devices-vs-more-virtual-experiences-and-technology-innovation-301919928.html

[3] Fortune Business Insights 2024. *Internet of Things [IoT] Market Size, Share, Growth, Trends, 2032*. Fortune Business Insights. Retrieved January 07, 2025 from https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

[4] Wikipedia 2024. *Laser Doppler vibrometer*. Wikipedia. Retrieved January 07, 2025 from https://en.wikipedia.org/wiki/Laser_Doppler_vibrometer#/media/File:LDV_Schematic.png

[5] Pew Research Center 2024. *Mobile Fact Sheet*. Pew Research Center. Retrieved January 07, 2025 from https://www.pewresearch.org/internet/fact-sheet/mobile/

[6] S Abhishek Anand and Nitesh Saxena. 2018. Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors. In *2018 IEEE Symposium on Security and Privacy (SP)*. 1000–1017. https://doi.org/10.1109/SP.2018.00004

[7] S Abhishek Anand, Chen Wang, Jian Liu, Nitesh Saxena, and Yingying Chen. 2021. Spearphone: a lightweight speech privacy exploit via accelerometer-sensed reverberations from smartphone loudspeakers. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Abu Dhabi, United Arab Emirates) *(WiSec '21)*. Association for Computing Machinery, New York, NY, USA, 288–299. https://doi.org/10.1145/3448300.3468499

[8] Zhongjie Ba, Tianhang Zheng, Xinyu Zhang, Zhan Qin, Baochun Li, Xue Liu, and Kui Ren. 2020. Learning-based Practical Smartphone Eavesdropping with Built-in Accelerometer. https://doi.org/10.14722/ndss.2020.24076

[9] Connor Bolton, Yan Long, Jun Han, Josiah Hester, and Kevin Fu. 2023. Characterizing and Mitigating Touchtone Eavesdropping in Smartphone Motion Sensors. In *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses* (Hong Kong, China) *(RAID '23)*. Association for Computing Machinery, New York, NY, USA, 164–178. https://doi.org/10.1145/3607199.3607203

[10] Eddy Bøgh Brixen. [n. d.]. *Facts about speech intelligibility*. DPA Microphones A/S. Retrieved January 07, 2025 from https://www.dpamicrophones.com/mic-university/background-knowledge/facts-about-speech-intelligibility/

[11] Liang Cai and Hao Chen. 2011. TouchLogger: inferring keystrokes on touch screen from smartphone motion. In *Proceedings of the 6th USENIX Conference on Hot Topics in Security* (San Francisco, CA) *(HotSec'11)*. USENIX Association, USA, 9.

[12] Wei-Han Chen and Kannan Srinivasan. 2022. Acoustic Eavesdropping from Passive Vibrations via mmWave Signals. In *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. 4051–4056. https://doi.org/10.1109/GLOBECOM48099.2022.10001108

[13] Yunzhong Chen, Jiadi Yu, Linghe Kong, Hao Kong, Yanmin Zhu, and Yi-Chao Chen. 2023. RF-Mic: Live Voice Eavesdropping via Capturing Subtle Facial Speech Dynamics Leveraging RFID. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 7, 2, Article 49 (June 2023), 25 pages. https://doi.org/10.1145/3596259

[14] Graham CLULEY. 2020. *Robot vacuum cleaners can eavesdrop on your conversations, researchers reveal*. Bitdefender. Retrieved January 07, 2025 from https://www.bitdefender.com/en-us/blog/hotforsecurity/robot-vacuum-cleaners-can-eavesdrop-conversations-researchers-reveal

[15] Ming Gao, Yajie Liu, Yike Chen, Yimin Li, Zhongjie Ba, Xian Xu, Jinsong Han, and Kui Ren. 2022. Device-Independent Smartphone Eavesdropping Jointly Using Accelerometer and Gyroscope. *IEEE Transactions on Dependable and Secure Computing* PP (01 2022), 1–14. https://doi.org/10.1109/TDSC.2022.3193130

[16] Jun Han, Albert Jin Chung, and Patrick Tague. 2017. PitchIn: eavesdropping via intelligible speech reconstruction using non-acoustic sensor fusion. In *Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks* (Pittsburgh, Pennsylvania) *(IPSN '17)*. Association for Computing Machinery, New York, NY, USA, 181–192. https://doi.org/10.1145/3055031.3055088

[17] Andrew Kwong, Wenyuan Xu, and Kevin Fu. 2019. Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone. In *2019 IEEE Symposium on Security and Privacy (SP)*. 905–919. https://doi.org/10.1109/SP.2019.00008

[18] Yunji Liang, Yuchen Qin, Qi Li, Xiaokai Yan, Zhiwen Yu, Bin Guo, Sagar Samtani, and Yanyong Zhang. 2022. AccMyrinx: Speech Synthesis with Non-Acoustic Sensor. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 3, Article 127 (Sept. 2022), 24 pages. https://doi.org/10.1145/3550338

[19] Richard Matovu, Isaac Griswold-Steiner, and Abdul Serwadda. 2019. Kinetic Song Comprehension: Deciphering Personal Listening Habits via Phone Vibrations. *CoRR* abs/1909.09123 (2019). arXiv:1909.09123 http://arxiv.org/abs/1909.09123

[20] Yan Michalevsky, Dan Boneh, and Gabi Nakibly. 2014. Gyrophone: recognizing speech from gyroscope signals. In *Proceedings of the 23rd USENIX Conference on Security Symposium* (San Diego, CA) *(SEC'14)*. USENIX Association, USA, 1053–1067.

Table 1: Test parameters and key results from previous publications on vibration-based speech recovery attacks exploiting different sensors

Year	Paper	Sensor	Measuring Device	Attack Goal	Sample Freq.	Audio source	Transmission Medium	Distance from source	Dictionary Size	Speech Rec. (best)
2014	Gyrophone [20]	Gyroscope	Android Smartphone	Speech Rec., Speaker Ident., Gender Ident.	200 Hz	External Loudspeaker	Solid Surface	10 cm	11 digits	26 %
2015	AccelWorld [29]	Accelerometer	Android Smartphone	Speech Rec., Speaker Ident.	200 Hz	External Loudspeaker	Air	30 cm	1 hotword	85 %
2017	PitchIn [16]	Accelerometer, Gyroscope, Geophone	Dedicated IMCU	Speech Rec.	1 kHz	Human	Air	1 m	10 words	79 %
2018	Speechless [6]	Accelerometer, Gyroscope	Android Smartphone	Speech Rec.	200 Hz	External Loudspeaker	Solid Surface	10 cm	10 digits	0 %
2019	Kinetic Song Comprehension [19]	Accelerometer, Gyroscope	Android Smartphone	Song Rec.	100 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	100 songs	80 %
2020	AccelEve [8]	Accelerometer	Android Smartphone	Speech Rec., Speaker Ident.	100-500 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	8 hotwords	90 %
2021	Spearphone [7]	Accelerometer	Android Smartphone	Speech Rec., Speaker Ident., Gender Ident.	120-500 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	58 words	67 %
2021	Vibphone [22]	Accelerometer	Android Smartphone	Speech Rec.	225-425 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	10 hotwords + 10 digits	54.2 %
2022	AccMyrinx [18]	Accelerometer	Android Smartphone	Speech Rec.	100-500 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	Synthesis	57.33 %
2022	InertiEAR [15]	Accelerometer, Gyroscope	Smartphone	Speech Rec.	40-200 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	10 digits	49.8 %
2023	ISpyU [30]	Accelerometer, Gyroscope	Android Smartphone	Automatic Speech Rec.	200-500 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	9950 words	53.3 %
2023	VoiceListener [24]	Accelerometer, Gyroscope, Magnetometer	Android Smartphone	Speech Rec.	100-500 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	10 digits	82.7 %
2023	StealthyIMU [23]	Accelerometer	Android Smartphone	Speech Rec. (Voice Assistant)	100-500 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	23 voice commands	-
2024	Watch the Rhythm [28]	Accelerometer	Android Smartphone	Speech Rec., Scene Rec.	5-200 Hz	Smartphone Loudspeaker	Solid Surface	On-Device	10 digits	77.79 %
2020	Lidarphone [21]	Lidar Scanner	Robot Vacuum Cleaner	Speech Rec., Song Rec., Speaker Ident., Gender Ident.	1.8 kHz	External Loudspeaker	Air	1.5 m	10 digits	91 %
2019	Hard Drive of Hearing [17]	Hard Drive PES	HDD Controller	Speech Rec., Song Rec.	34.56 kHz	External Loudspeaker	Air	25 cm	-	100 %

[21] Sriram Sami, Sean Rui Xiang Tan, Yimin Dai, Nirupam Roy, and Jun Han. 2020. LidarPhone: acoustic eavesdropping using a lidar sensor: poster abstract. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems* (Virtual Event, Japan) *(SenSys '20)*. Association for Computing Machinery, New York, NY, USA, 701–702. https://doi.org/10.1145/3384419.3430430

[22] Weigao Su, Daibo Liu, Taiyuan Zhang, and Hongbo Jiang. 2022. Towards Device Independent Eavesdropping on Telephone Conversations with Built-in Accelerometer. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 177 (Dec. 2022), 29 pages. https://doi.org/10.1145/3494969

[23] Ke Sun, Chunyu Xia, Songlin Xu, and Xinyu Zhang. 2023. StealthyIMU: Stealing Permission-protected Private Information From Smartphone Voice Assistant Using Zero-Permission Sensors. https://doi.org/10.14722/ndss.2023.24077

[24] Lei Wang, Meng Chen, Li Lu, Zhongjie Ba, Feng Lin, and Kui Ren. 2023. VoiceListener: A Training-free and Universal Eavesdropping Attack on Built-in Speakers of Mobile Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 7, 1, Article 32 (March 2023), 22 pages. https://doi.org/10.1145/3580789

[25] Teng Wei, Shu Wang, Anfu Zhou, and Xinyu Zhang. 2015. Acoustic Eavesdropping through Wireless Vibrometry. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking* (Paris, France) *(MobiCom '15)*. Association for Computing Machinery, New York, NY, USA, 130–141. https://doi.org/10.1145/2789168.2790119

[26] Davey Winder. 2020. *Hacked Vacuum Cleaner Can Record Your Conversations—No Microphone Required.* Forbes. Retrieved January 07, 2025 from https://www.forbes.com/sites/daveywinder/2020/11/22/how-this-hacked-vacuum-cleaner-can-listen-to-your-conversations-using-lidar

[27] Zhi Xu, Kun Bai, and Sencun Zhu. 2012. TapLogger: inferring user inputs on smartphone touchscreens using on-board motion sensors. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Tucson, Arizona, USA) *(WISEC '12)*. Association for Computing Machinery, New York, NY, USA, 113–124. https://doi.org/10.1145/2185448.2185465

[28] Qingsong Yao, Yuming Liu, Xiongjia Sun, Xuewen Dong, Xiaoyu Ji, and Jianfeng Ma. 2024. Watch the Rhythm: Breaking Privacy with Accelerometer at the Extremely-Low Sampling Rate of 5Hz. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1776–1790. https://doi.org/10.1145/3658644.3690370

[29] Li Zhang, Parth H. Pathak, Muchen Wu, Yixin Zhao, and Prasant Mohapatra. 2015. AccelWord: Energy Efficient Hotword Detection through Accelerometer. In *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services* (Florence, Italy) *(MobiSys '15)*. Association for Computing Machinery, New York, NY, USA, 301–315. https://doi.org/10.1145/2742647.2742658

[30] Shijia Zhang, Yilin Liu, and Mahanth Gowda. 2023. I Spy You: Eavesdropping Continuous Speech on Smartphones via Motion Sensors. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 4, Article 197 (Jan. 2023), 31 pages. https://doi.org/10.1145/3569486

Received 7 January 2025