black hat ASIA 2021
May 6-7, 2021
BRIEFINGS

The Motion Sensor Western

Ben Nassi

Ph.D. Student, Ben-Gurion University of the Negev

About Me

Cyber@Ben-Gurion University of the Negev | Israel National Cyber Bureau

Cyber Security Research Center

Computer Scientist & Former Google Employee

Ph.D. Student @ Ben-Gurion University of the Negev, Israel

Researcher at CBG (Cyber @ BGU)

Research Focus:

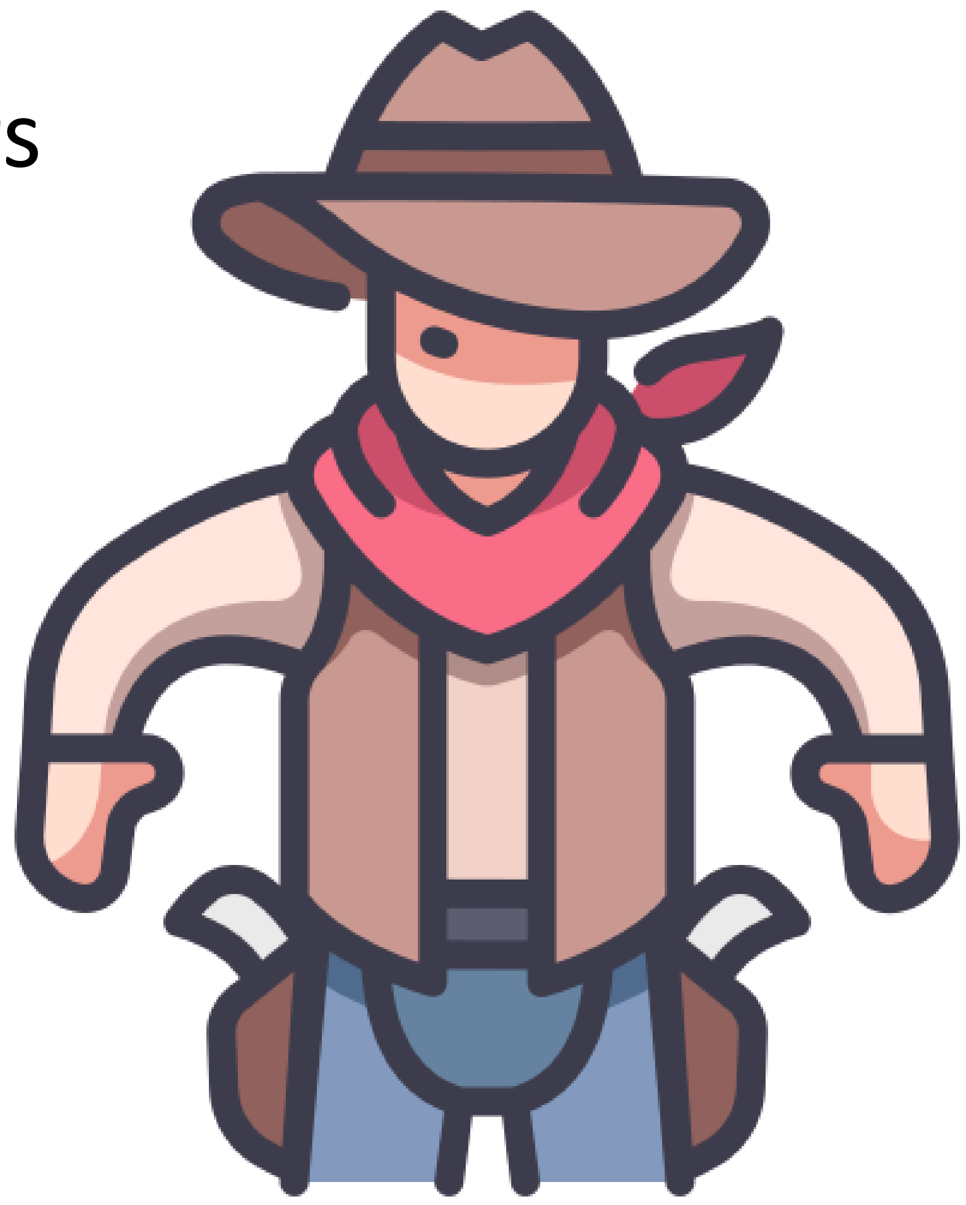
- Side-channel attacks
- Sound recovery via non-acoustic data
- Security of autonomous vehicles (drones, advanced driver-assistance systems)

@ben_nassi

Read more about my research at www.nassiben.com.

Agenda

- The Good: Advantages of Motion Sensors
- The Bad: Security Risks
- The Ugly: Privacy Risks
  - User study
- Takeaways
- Q&A



The Good

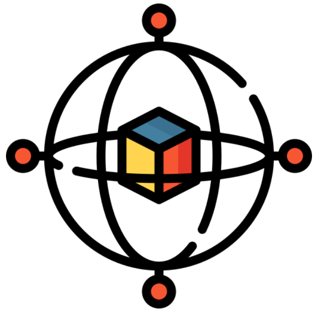
MEMS Motion Sensors

MEMS (Micro-Electro-Mechanical Systems) motion sensors are electrical devices that utilize a sensor to detect nearby motion.

In this talk we focus on two specific motion sensors

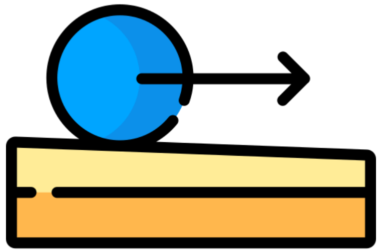
MEMS Gyroscope

A device which is used to measure the angular velocity



MEMS Accelerometer

A device which is used to measure the rate of change of a velocity.



Advantages

Cheap

Advantages

Cheap

Provide sufficient accuracy

Advantages

Cheap

Provide sufficient accuracy

Low power consumption

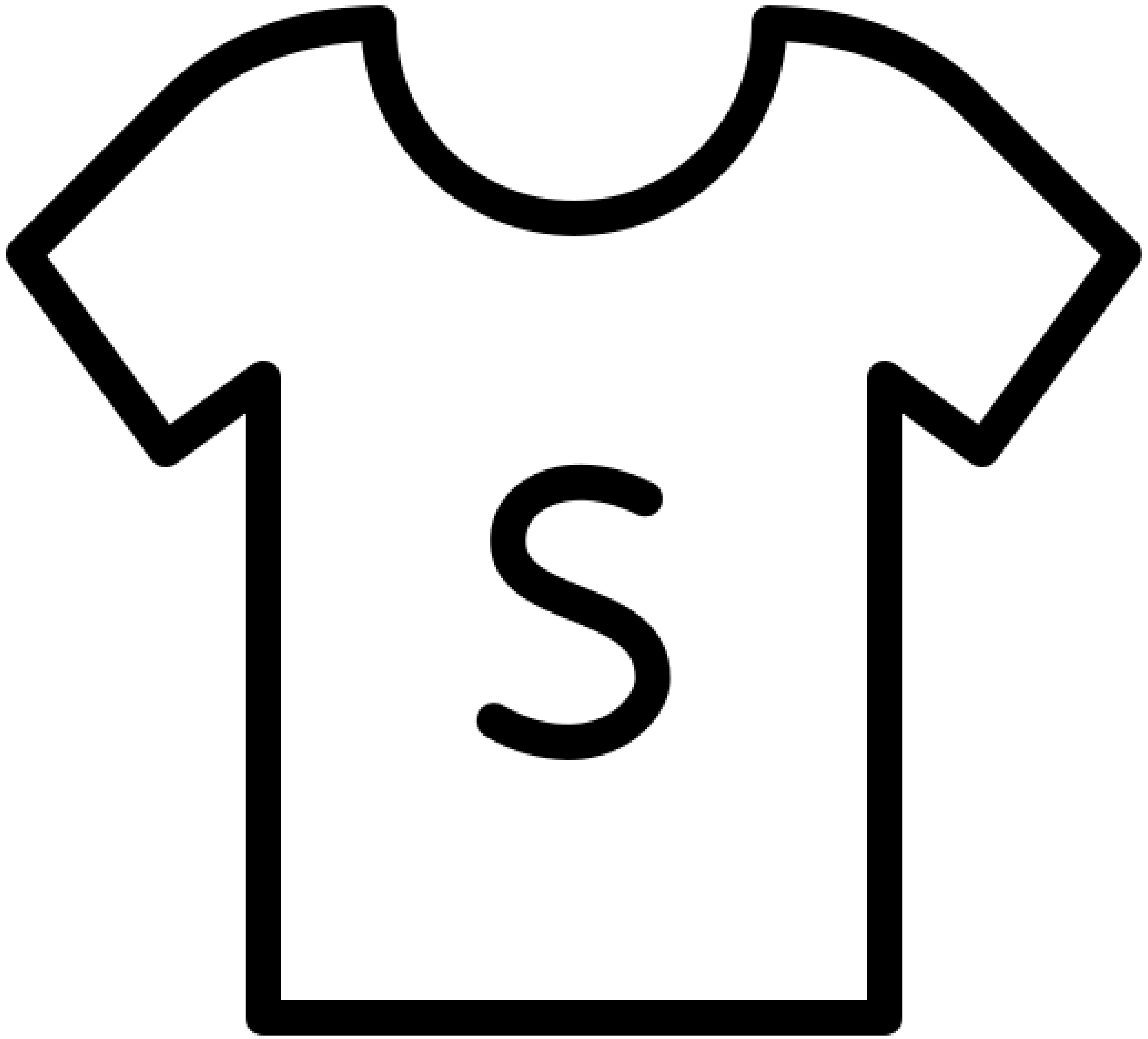
Advantages

Cheap

Provide sufficient accuracy

Low power consumption

Small



Use

Motion sensors have become more and more ubiquitous.

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Smartphones & Tablets

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Smartphones & Tablets

Smartwatches & Fitness Trackers

Use

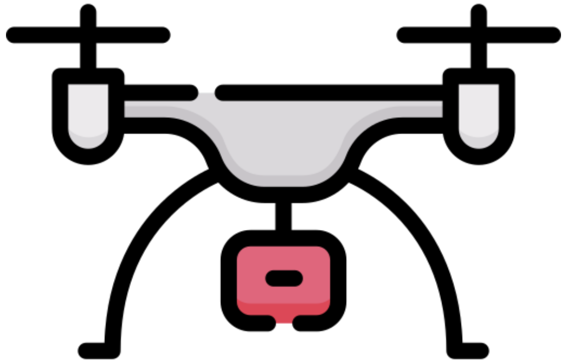
Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Smartphones & Tablets

Smartwatches & Fitness Trackers

Drones



Use

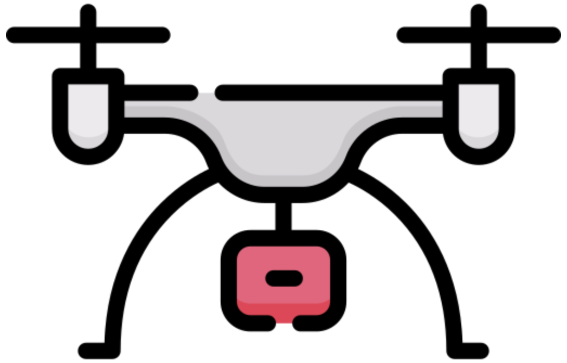
Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Smartphones & Tablets

Smartwatches & Fitness Trackers

Drones



Headphones

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

Real-time automatic user gesture recognition (smartphones)

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

- Real-time automatic user gesture recognition (smartphones)
- **Real-time automatic stabilization (drones, GoPro cameras)**

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

- Real-time automatic user gesture recognition (smartphones)
- Real-time automatic stabilization (drones, GoPro cameras)
- **Improved gaming experience (turning a smartphone into a joystick)**

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

- Real-time automatic user gesture recognition (smartphones)
- Real-time automatic stabilization (drones, GoPro cameras)
- Improved gaming experience (turning a smartphone into a joystick)
- **Real-time user activity recognition (detecting walking)**

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

- Real-time automatic user gesture recognition (smartphones)
- Real-time automatic stabilization (drones, GoPro cameras)
- Improved gaming experience (turning a smartphone into a joystick)
- Real-time user activity recognition (detecting walking)
- **User health monitoring (counting steps)**

Use

Motion sensors have become more and more ubiquitous.

They are integrated in many IoT devices.

Their data is used for various tasks:

- Real-time automatic user gesture recognition (smartphones)
- Real-time automatic stabilization (drones, GoPro cameras)
- Improved gaming experience (turning a smartphone into a joystick)
- Real-time user activity recognition (detecting walking)
- User health monitoring (counting steps)
- **Navigation (IMU)**

Use

Motion sensors have become more and more ubiquitous.
They are integrated in many IoT devices.

Most everyone in the audience is being sampled by motion sensors in at least one device for most of the day.

The Bad

Security of Devices

The Vulnerability

In 2007, resonant acoustic injection frequency attack was identified as a problem that causes performance degradation of MEMS motion sensors [1] [2].

The Vulnerability

In 2007, resonant acoustic injection frequency was identified as a problem that causes performance degradation of MEMS motion sensors [1] [2].

Most MEMS gyroscopes [3] and accelerometers [4] have a unique resonant frequency that is related to the physical characteristics of their structure.

The Vulnerability

As a result of this resonance, MEMS motion sensors generate an unexpected output that may cause the related systems to malfunction in response to sound played at their resonant frequency.

The Vulnerability

As a result of this resonance, MEMS motion sensors generate an unexpected output that may cause the related systems to malfunction in response to sound played at their resonant frequency.

These resonant frequencies are often considered to be commercial secrets.

The Vulnerability

As a result of this resonance, MEMS motion sensors generate an unexpected output that may cause the related systems to malfunction in response to sound played at their resonant frequency.

These resonant frequencies are often considered to be commercial secrets.

Resonant frequency ranges

for MEMS gyroscopes: 7.9-28.6 KHz

for MEMS accelerometers: 2.2-13 KHz

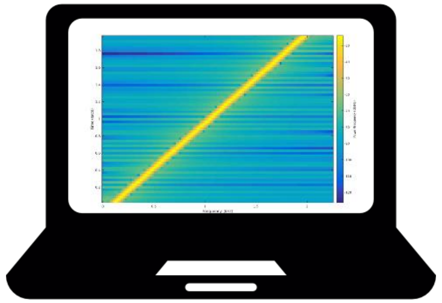
The Vulnerability

How attackers can find/identify the resonant frequency of a motion sensor?

Resonant Acoustic Injection Frequency Attack

Given a motion sensor, the range around the resonance frequency can be detected as follows:

Produce a signal of a frequency scan (chirp).

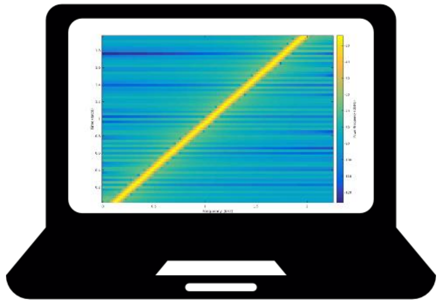


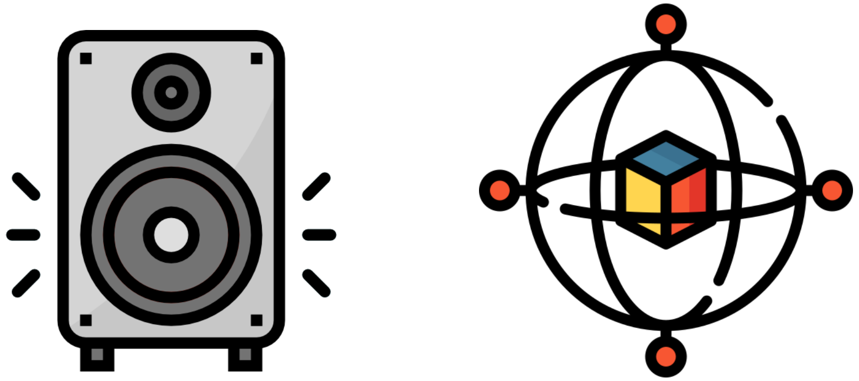
Resonant Acoustic Injection Frequency Attack

Given a motion sensor, the range around the resonance frequency can be detected as follows:

Produce a signal of a frequency scan (chirp).

Play the signal via speakers in proximity to the motion sensor.

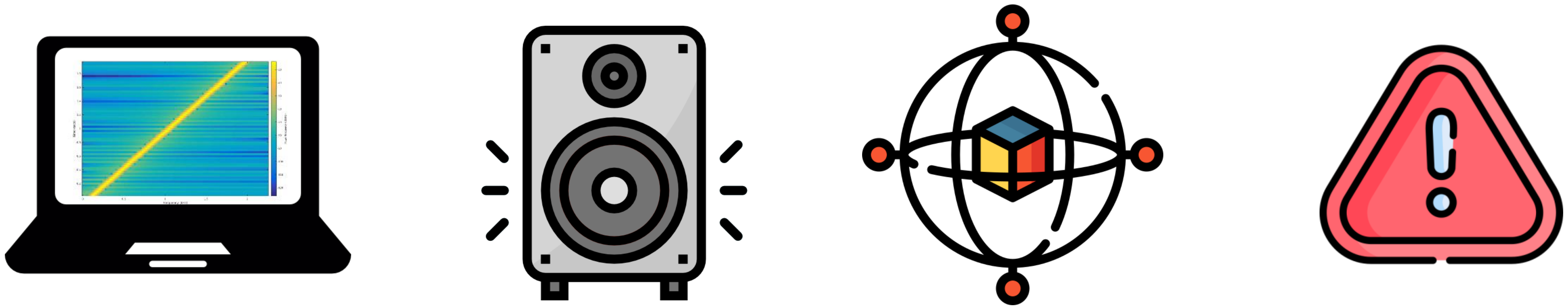




Resonant Acoustic Injection Frequency Attack

Given a motion sensor, the range around the resonance frequency can be detected as follows:

- Produce a signal of a frequency scan (chirp).
- Play the signal via speakers in proximity to the motion sensor.
- **Look for anomalies in the output of the motion sensor or the behavior of the containing device and identify the resonant frequency.**

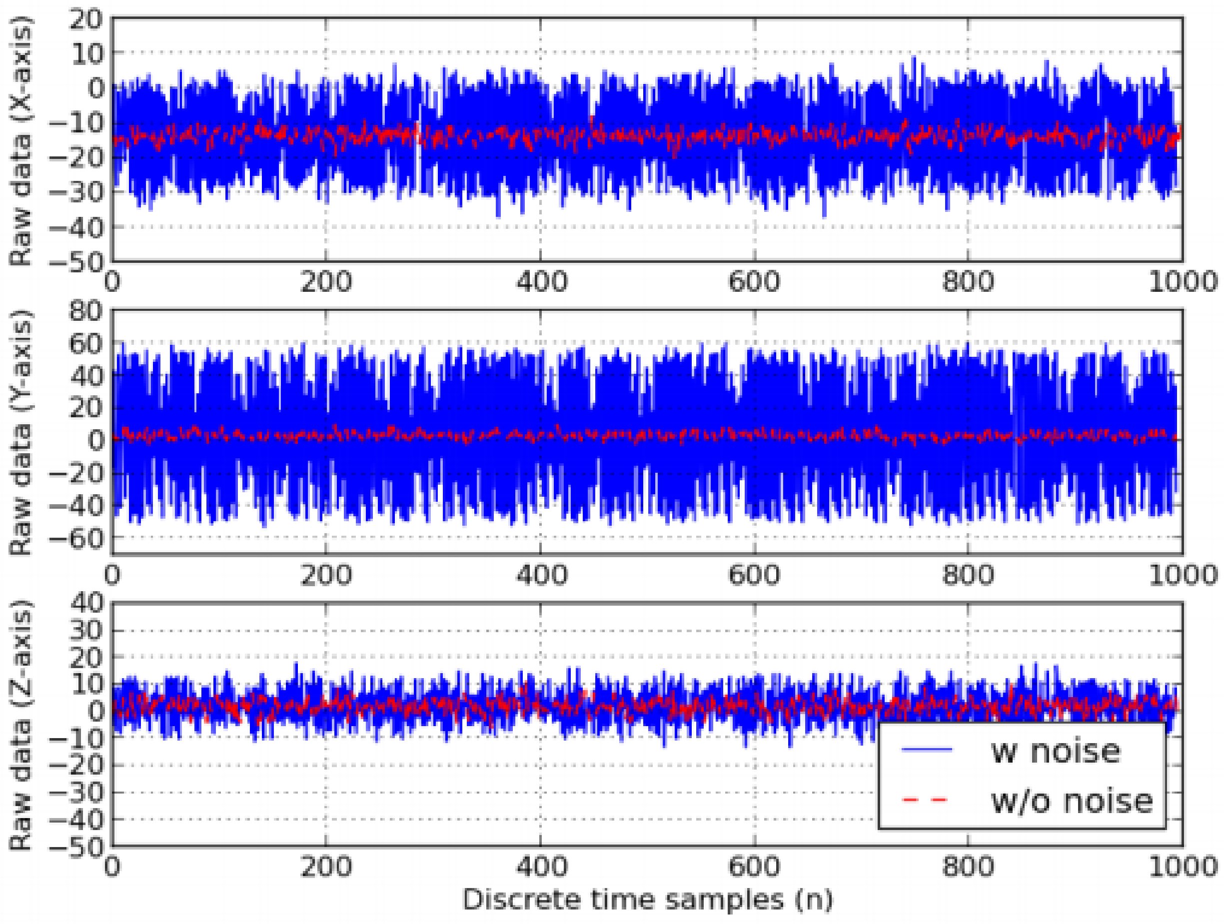


Resonant Acoustic Injection Frequency Attack

What are the anomalies that attackers need to look for when they apply the resonant acoustic injection frequency attack?

Resonant Acoustic Injection Frequency Attack

The picture on the right side shows how the original output of a gyroscope (in red) was changed in response to the attack (in blue)



(d) Raw data samples of one L3G4200D chip with the single tone sound noise at 8,000Hz

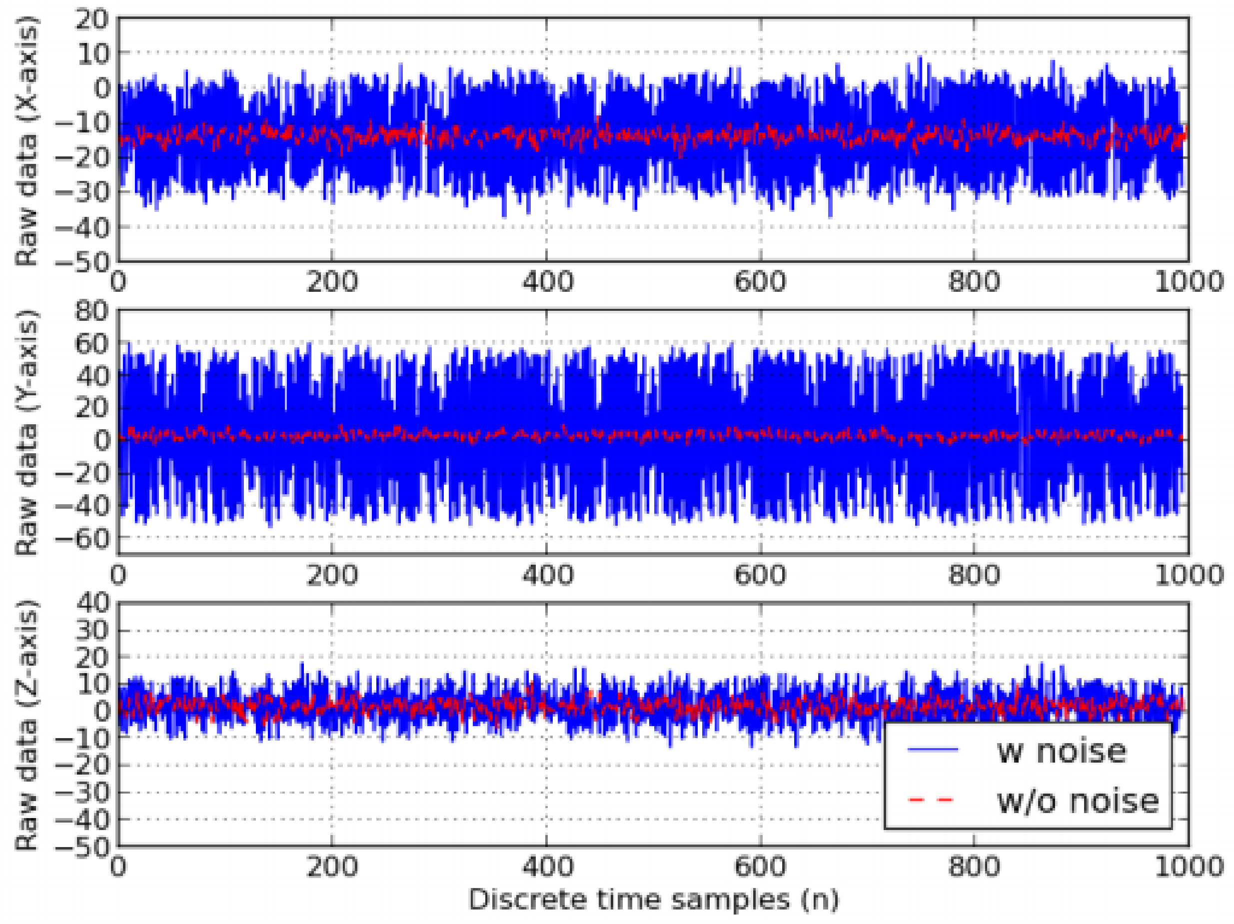
Pictures are courtesy of Son et al.

Resonant Acoustic Injection Frequency Attack

The picture on the right side shows how the original output of a gyroscope (in red) was changed in response to the attack(in blue)

In some cases, the attack increases the output's:

- **Standard deviation**
- **Range**
- **The absolute minimum/maximum values**

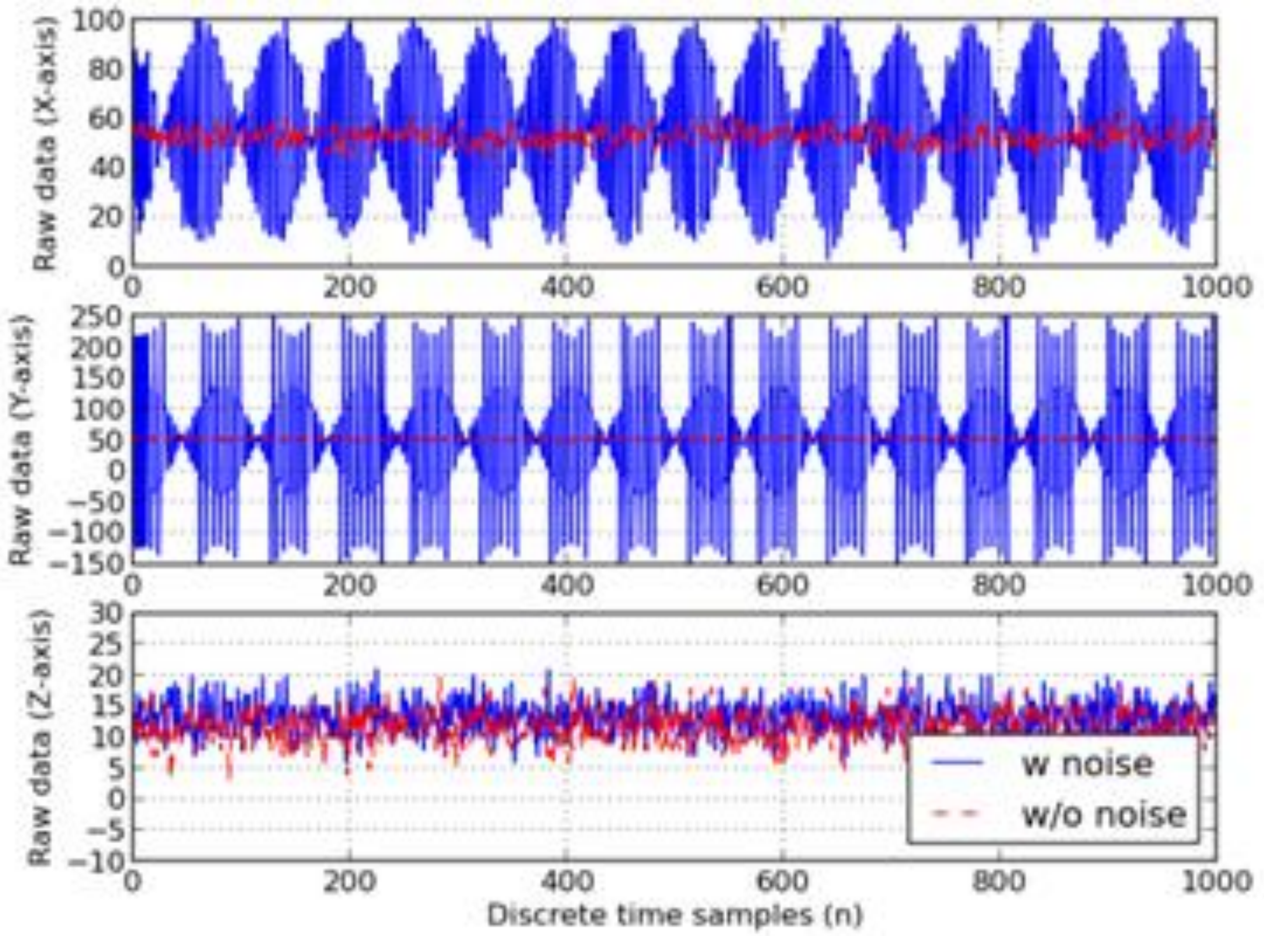


(d) Raw data samples of one L3G4200D chip with the single tone sound noise at 8,000Hz

Pictures are courtesy of Son et al.

Resonant Acoustic Injection Frequency Attack

In other cases (as can be seen in the picture on the right), the attack completely distorts the original signal.



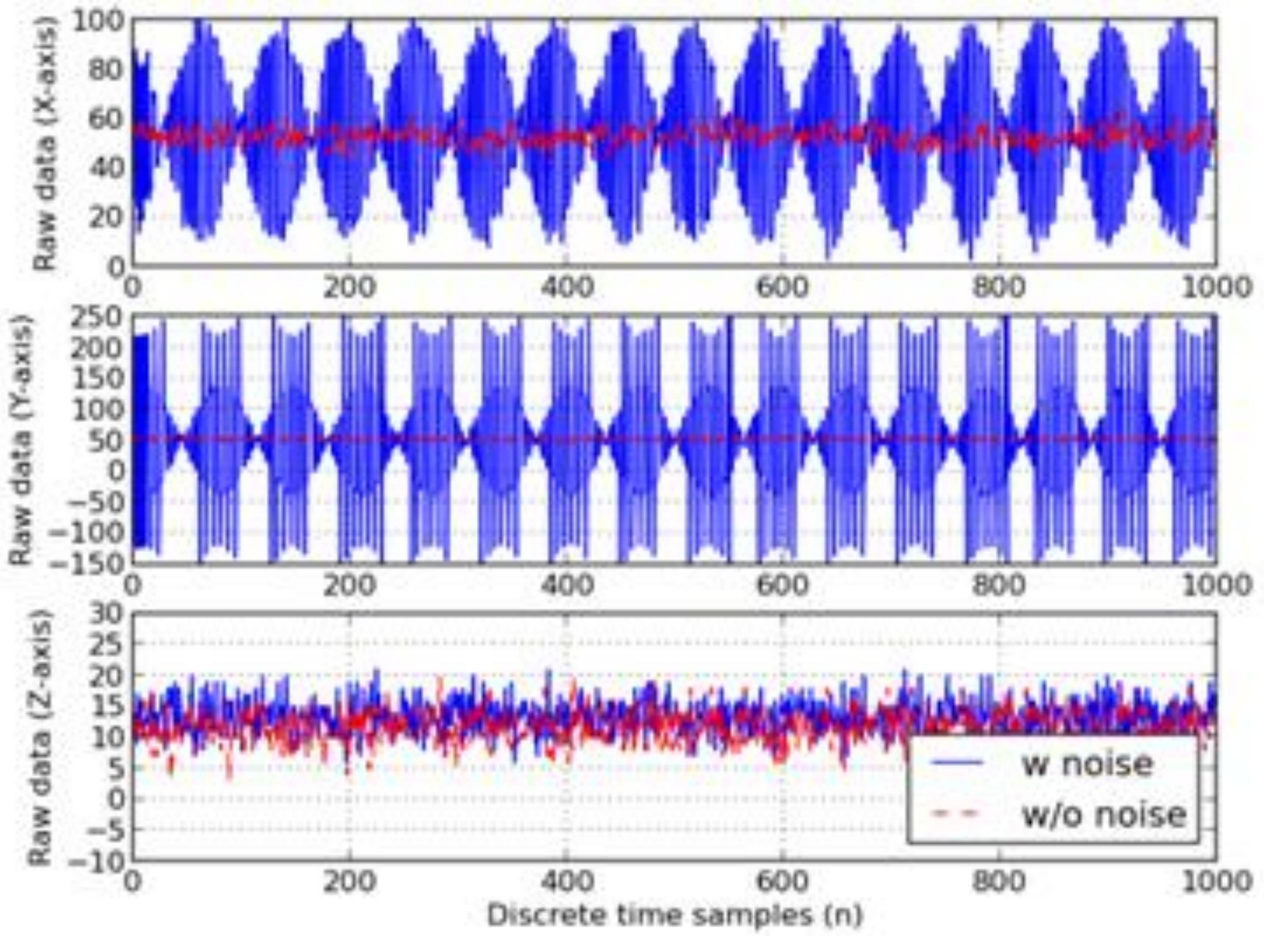
(a) Raw data samples of one L3GD20 chip with a single-tone sound noise at 20,100Hz

Pictures are courtesy of Son et al.

Resonant Acoustic Injection Frequency Attack

In other cases (as can be seen in the picture on the right), the attack completely distorts the original signal.

By applying the attack, attackers can control the output of a motion sensor.



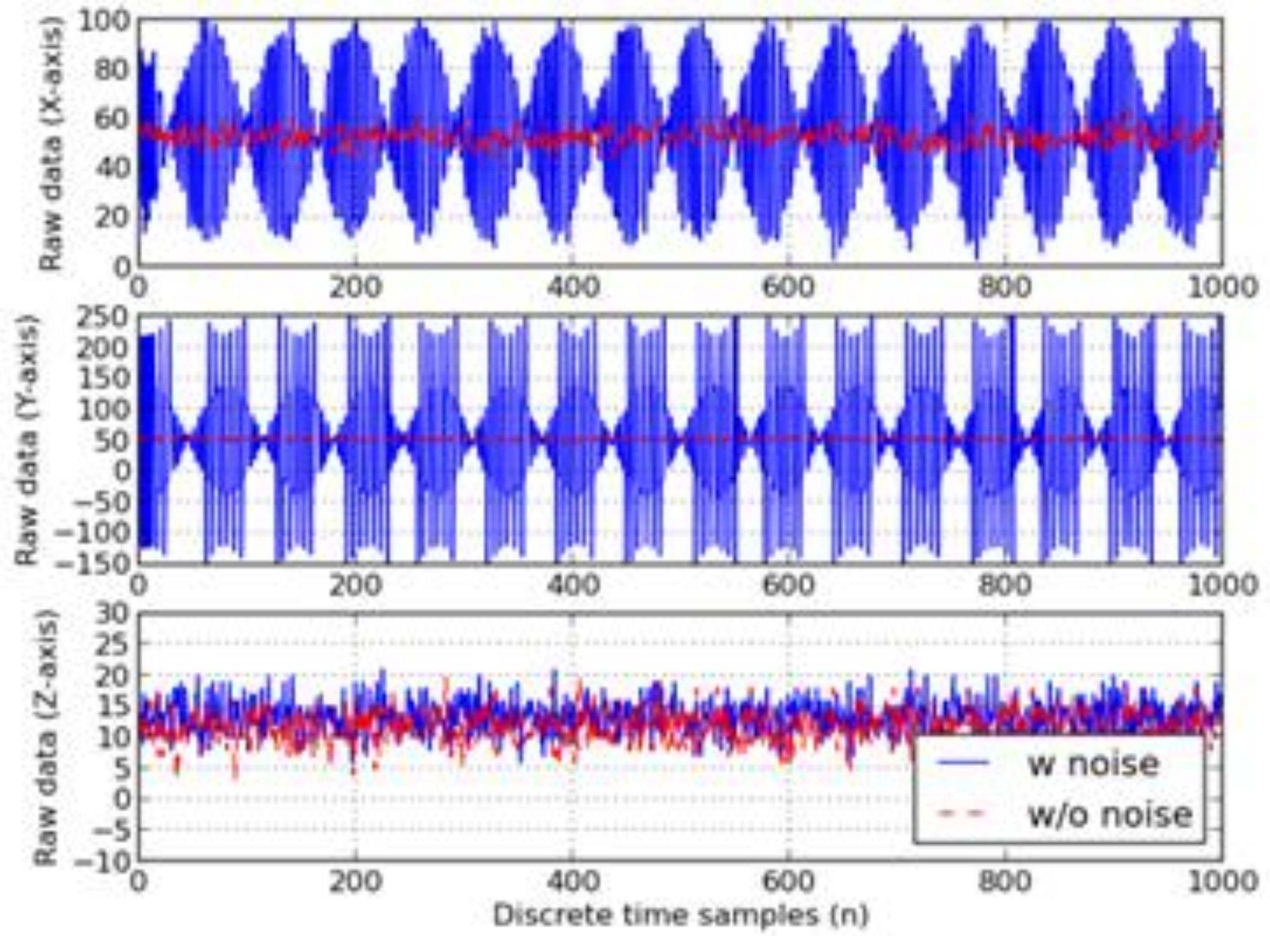
(a) Raw data samples of one L3GD20 chip with a single-tone sound noise at 20,100Hz

Pictures are courtesy of Son et al.

Resonant Acoustic Injection Frequency Attack

In other cases (as can be seen in the picture on the right), the attack completely distorts the original signal.

By applying the attack, attackers can control the output of a motion sensor.



These results clearly show that attackers can spoof the output of a target motion sensor, and affect the algorithms that rely on the motion sensor output.

et al.

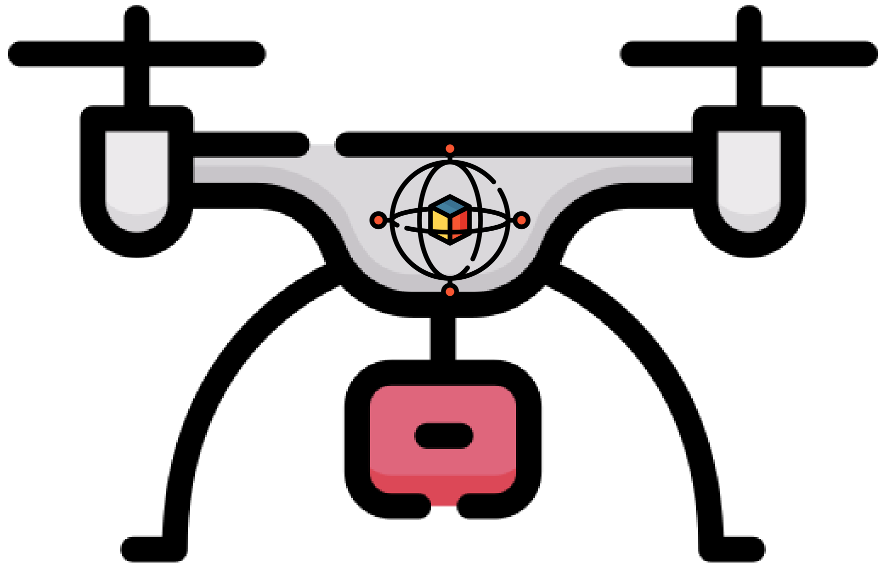
Question

Question: Given that the resonant frequency of a motion sensor is known, what are the risks that the resonant acoustic injection frequency attack poses to devices?

Attacking a Drone's Availability

Gyroscope are integrated in drones' IMUs.

The drone is a real-time system that continuously uses a gyroscope's measurements to stabilize itself while flying:



While (true){

x,y,z <- obtain gyroscope measurements.

Stabilize the drone by adjusting the copters' velocity according to x,y,z.

}

Attacking a Drone's Availability

Gyroscope are integrated in drones' IMUs.

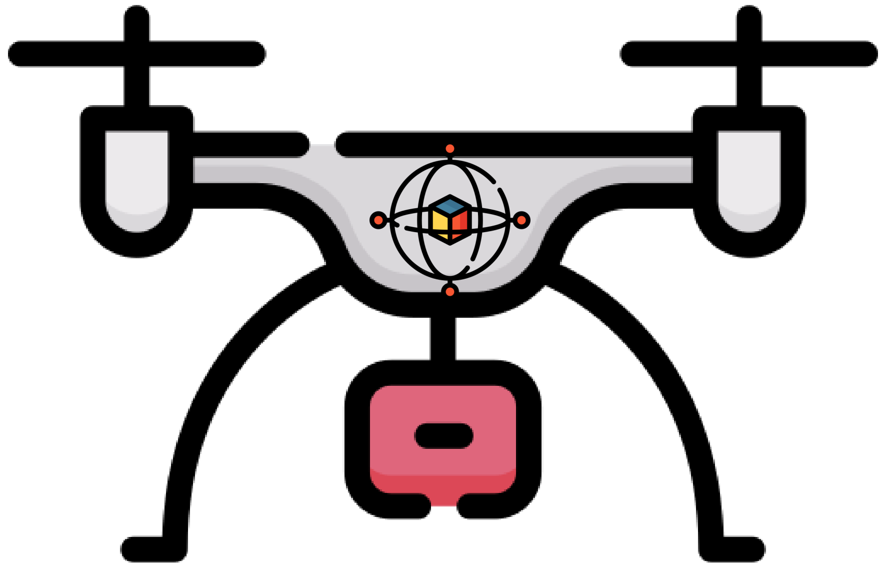
The drone is a real-time system that continuously uses a gyroscope's measurements to stabilize itself while flying:

While (true){

x,y,z <- obtain gyroscope measurements.

Stabilize the drone by adjusting the copters' velocity according to x,y,z.

}



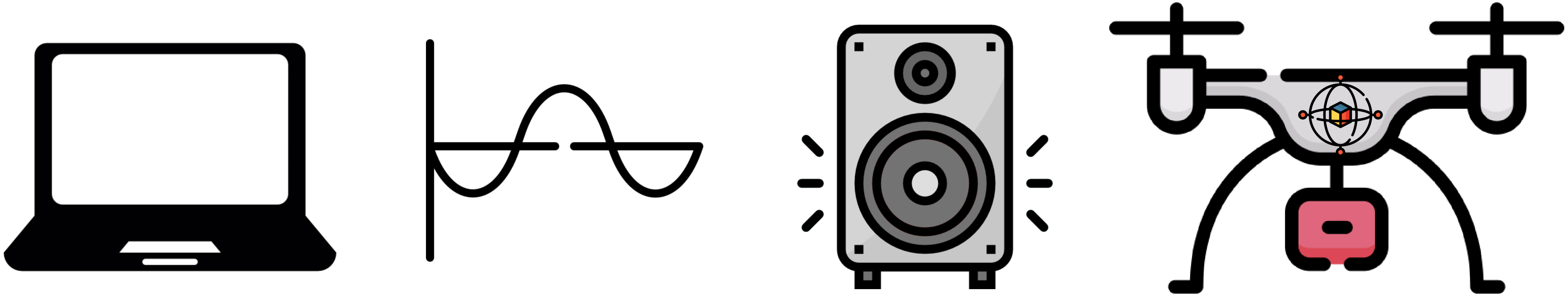
This procedure is executed a few times on each second by a drone's OS

Attacking a Drone’s Availability

In 2016, a group of scientists demonstrated a new technique aimed at interfering with a drone flight

Attacking a Drone’s Availability

In 2016, a group of scientists from demonstrated a new technique aimed at interfering with a drone flight



By applying the resonant acoustic injection frequency attack against drones, attackers were able to apply a DoS attack: (1) preventing a drone on the ground from ascending, and (2) crashing a flying drone.

Attacking a Drone’s Availability

Picture is courtesy of Son et al.

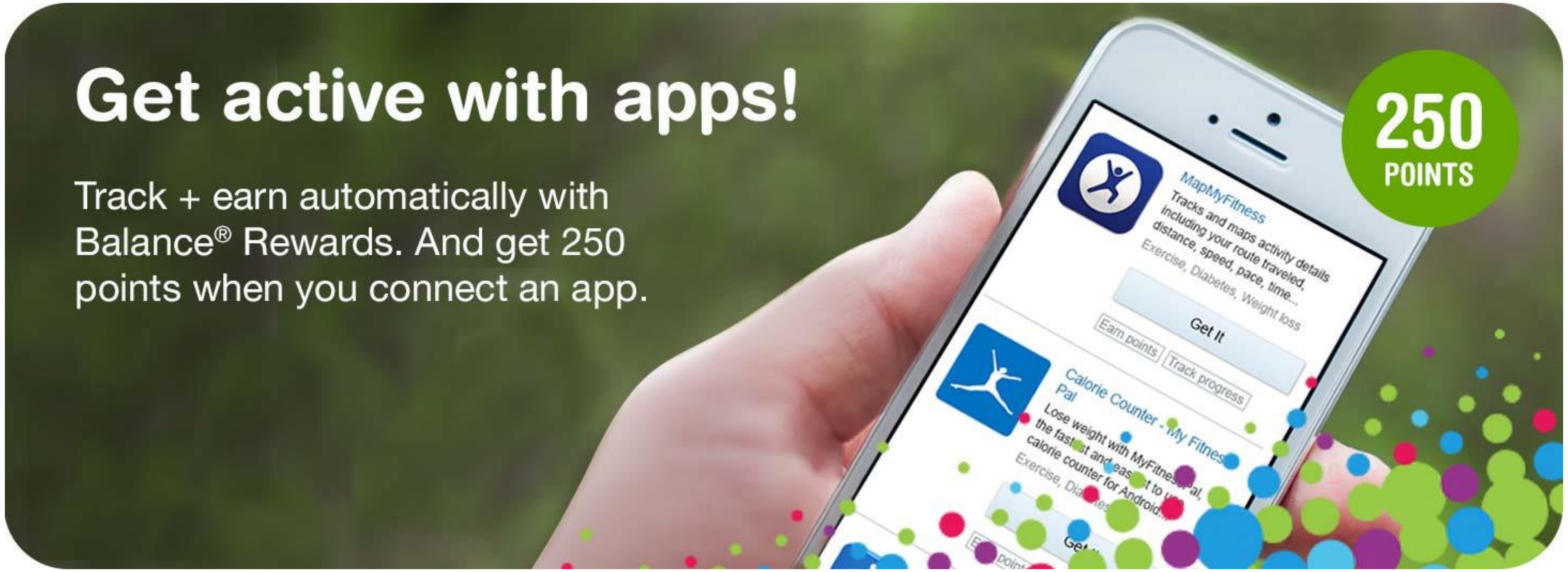
Attacking a Smartwatch’s Integrity

Accelerometers are integrated in smartwatches and fitness trackers.

Accelerometers are used to track many of the activities performed by the user, e.g., step counting.

Many companies incentivize people to exercise by offering reward programs tied to their personal fitness tracking wristbands.

Attacking a Smartwatch's Integrity



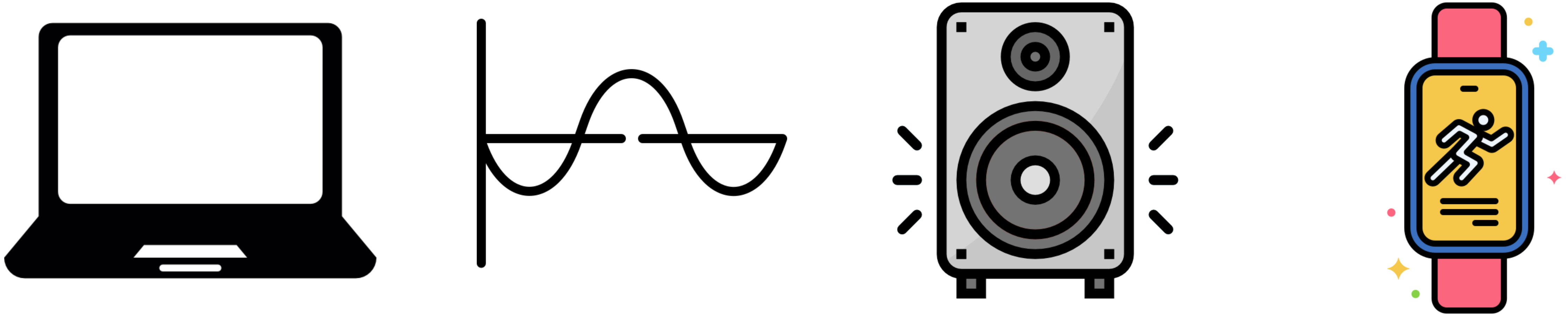
A user can earn free points by reaching a daily target of steps.

Attacking a Smartwatch’s Integrity

In 2017, a group of scientists [4] demonstrated a new technique to spoof the step counter

Attacking a Smartwatch's Integrity

In 2017, a group of scientists [4] demonstrated a new technique to spoof the step counter



By applying 40 minutes of the resonant acoustic injection frequency attack against the fitness tracker, attackers were able to register 2,100 steps and earn 21 reward points on Higi.com without taking a single step.

Summary

The availability and integrity of devices with integrated motion sensors can be violated by resonant acoustic injection frequency attack.

Summary

The availability and integrity of devices with integrated motion sensors can be violated by resonant acoustic injection frequency attack.

Spoofing a device with motion sensors requires the attacker to place the speakers in proximity to the attacked device, because sound deteriorates significantly with distance.

Summary

The availability and integrity of devices with integrated motion sensors can be violated by resonant acoustic injection frequency attack.

Spoofing a device with motion sensors requires the attacker to place the speakers in proximity to the attacked device, because sound deteriorates significantly with distance.

Conclusions:

The feasibility of this attack is highly dependent on the attacked device and the reality of the threat model.

Summary

The availability and integrity of devices with integrated motion sensors can be violated by resonant acoustic injection frequency attack.

Spoofing a device with motion sensors requires the attacker to place the speakers in proximity to the attacked device, because sound deteriorates significantly with distance.

Conclusions:

- The feasibility of this attack is highly dependent on the attacked device and the reality of the threat model.
- **The good news: In some cases, the attack is not considered a practical threat (e.g., crashing a flying drone used for deliveries) because it is hard to apply the attack from great distances.**

Summary

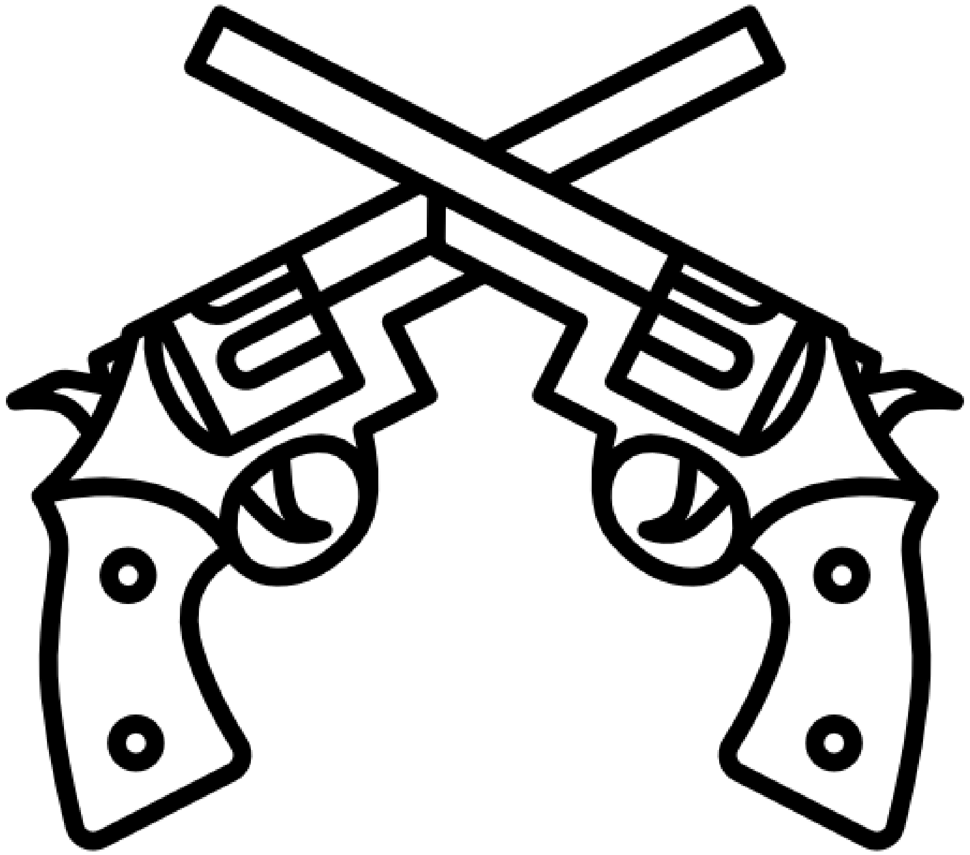
The availability and integrity of devices with integrated motion sensors can be violated by resonant acoustic injection frequency attack.

Spoofing a device with motion sensors requires the attacker to place the speakers in proximity to the attacked device, because sound deteriorates significantly with distance.

Conclusions:

- The feasibility of this attack is highly dependent on the attacked device and the reality of the threat model.
- The good news: In some cases, the attack is not considered a practical threat (e.g., crashing a flying drone used for deliveries), because it is hard to apply the attack from great distances.
- **The bad news: In other cases, the attack is considered a practical threat (e.g., spoofing the step counter of a smartwatch), because attackers can attack their own devices.**

The Ugly



Privacy of Individuals

Privacy Issues in Smartphones and Smartwatches

Motion sensors are integrated in smartphones and smartwatches.

Privacy Issues in Smartphones and Smartwatches

Motion sensors are integrated in smartphones and smartwatches.

Smartphones and smartwatches are carried almost 24/7 by their users.

Privacy Issues in Smartphones and Smartwatches

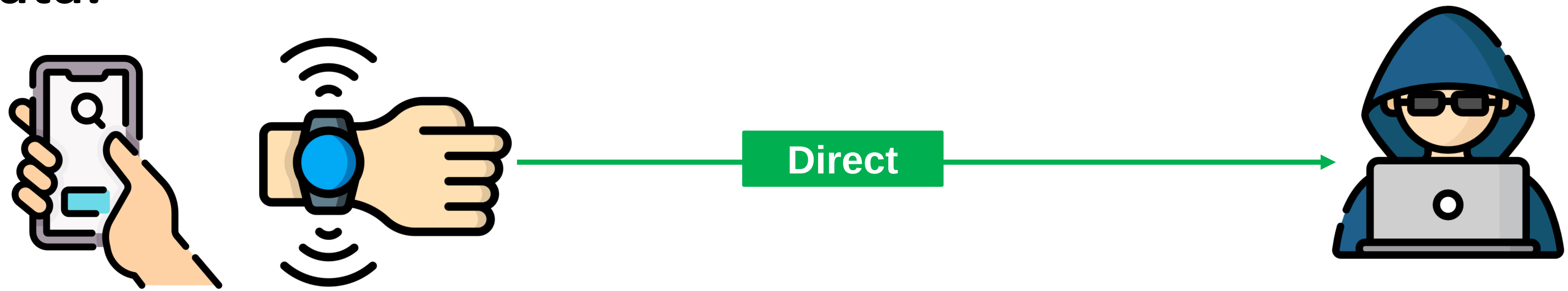
Motion sensors are integrated in smartphones and smartwatches.

Smartphones and smartwatches are carried almost 24/7 by their users.

Question: How can attackers obtain motion sensor data?

Threat Model

There are two ways that attackers can obtain motion sensor data:

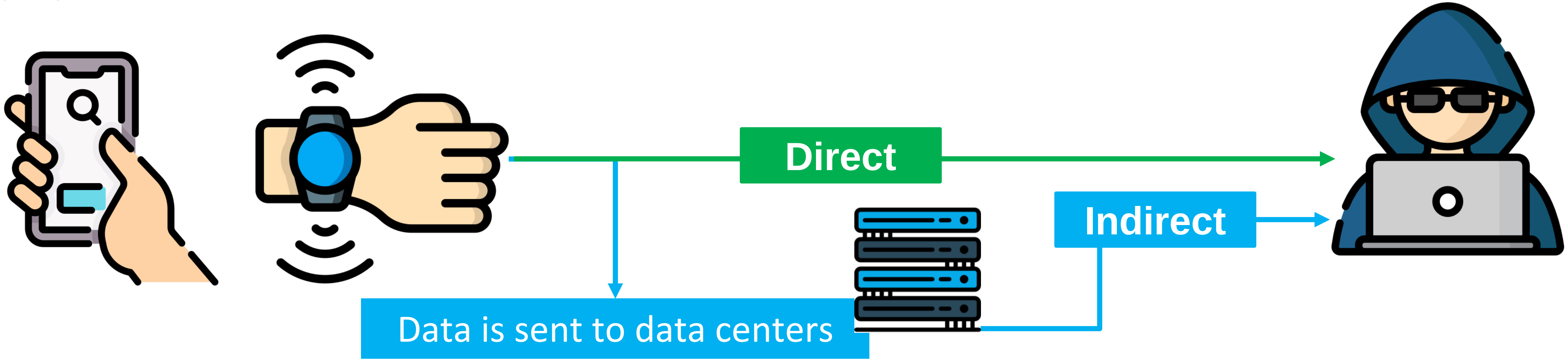


<u>Attackers can obtain data **directly** from these devices</u>

- By sampling the motion sensor via the browser when a user visits a compromised website.
- By sampling the motion sensor via an installed malicious application.
- By sampling the motion sensor via a malicious SDK integrated in a legitimate application.

Threat Model

There are two ways that attackers can obtain motion sensor data:

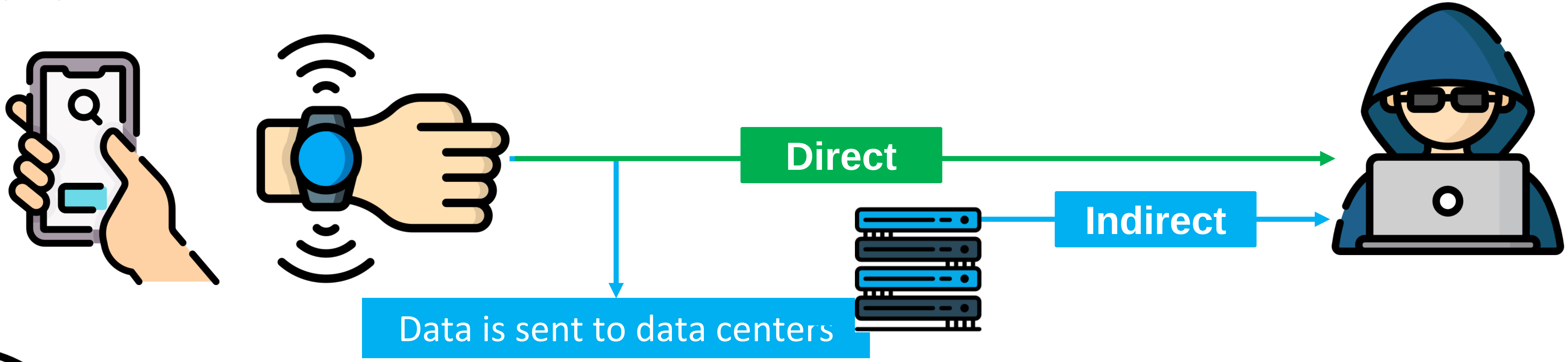


Attackers can obtain data **directly** from these devices
- By sampling the motion sensor via the browser when a user visits a compromised website.
- By sampling the motion sensor via an installed malicious application.
- By sampling the motion sensor via a malicious SDK integrated in a legitimate application.

Attackers can obtain data **indirectly**
- By hacking a legitimate application's data center.

Threat Model

There are two ways that attackers can obtain motion sensor data:



Question: Assuming that attackers were able to obtain motion sensor data, what are the risks that this data poses to individuals?

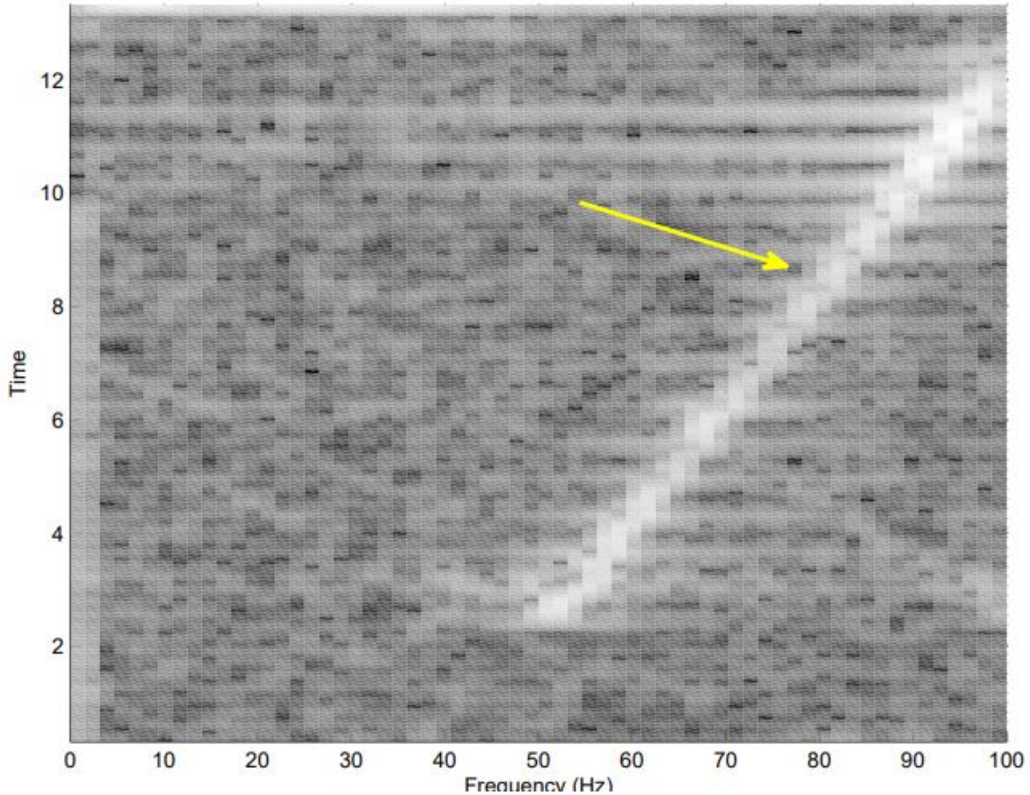
Recovering Sound from Motion Sensors

<u>Case study 1</u>

Question: Can motion sensors data be used to recover speech?

Recovering Sound from Motion Sensors

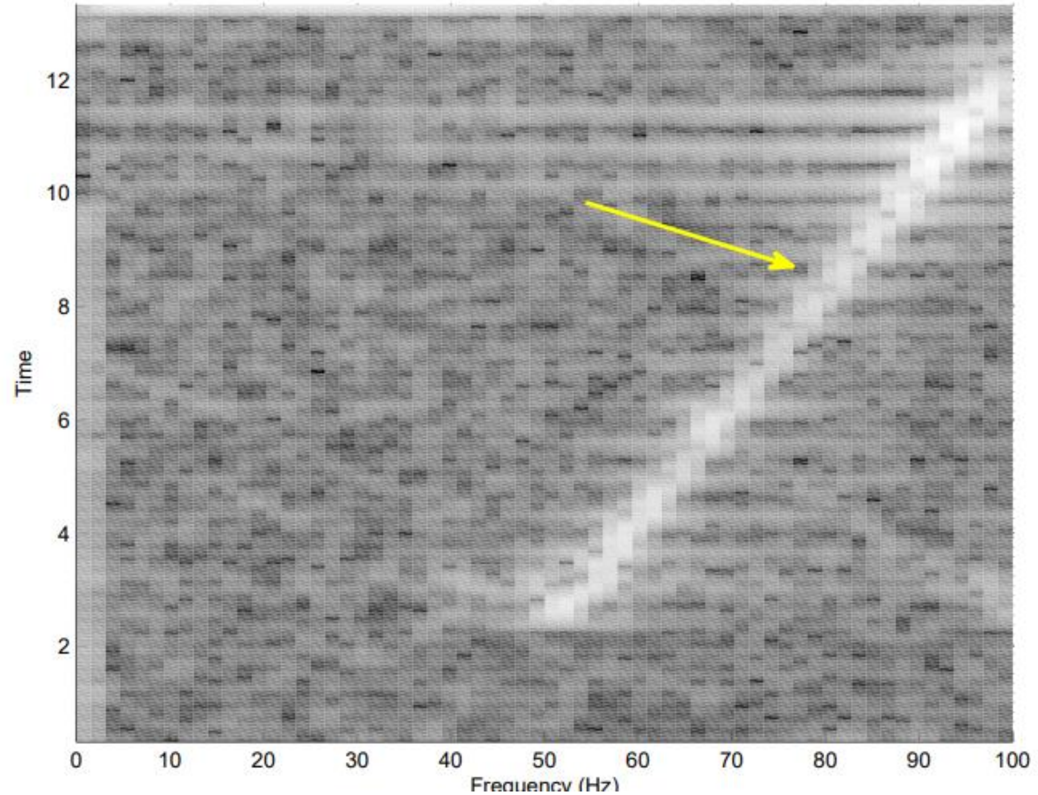
At USENIX Security 14, a group of scientists found that gyroscopes also capture acoustics.



Recovering Sound from Motion Sensors

At USENIX Security 14, a group of scientists found that gyroscopes also capture acoustics.

They were able to classify words by analyzing gyroscope data.



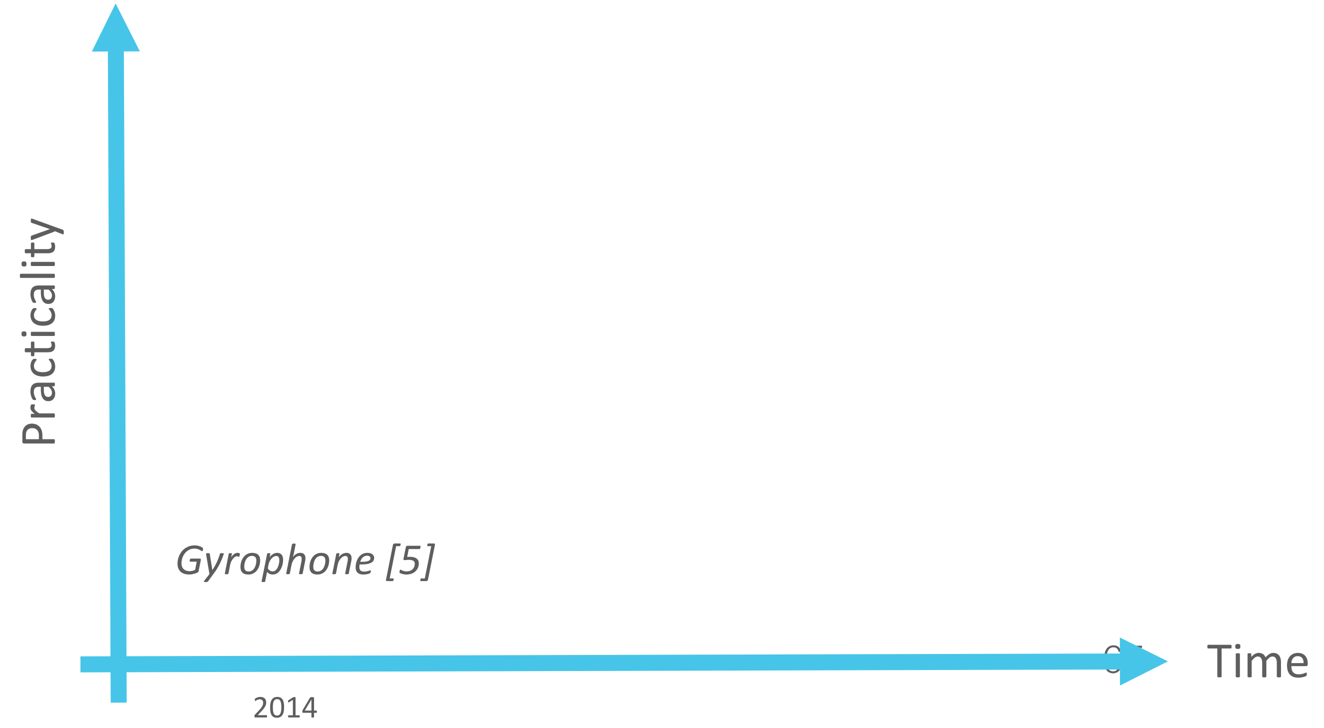
Recovering Sound from Motion Sensors

At USENIX Security 14, a group of scientists found that gyroscopes also capture acoustics.

They were able to classify words by analyzing gyroscope data.

In 2014, the attack was considered impractical:

- A smartphone OS limits the sampling rate from the gyroscope to 200 Hz.
- As a result, the accuracy of the model (KNN) was only slight better than a random guess.
- The attack vector relied on a very loud speech



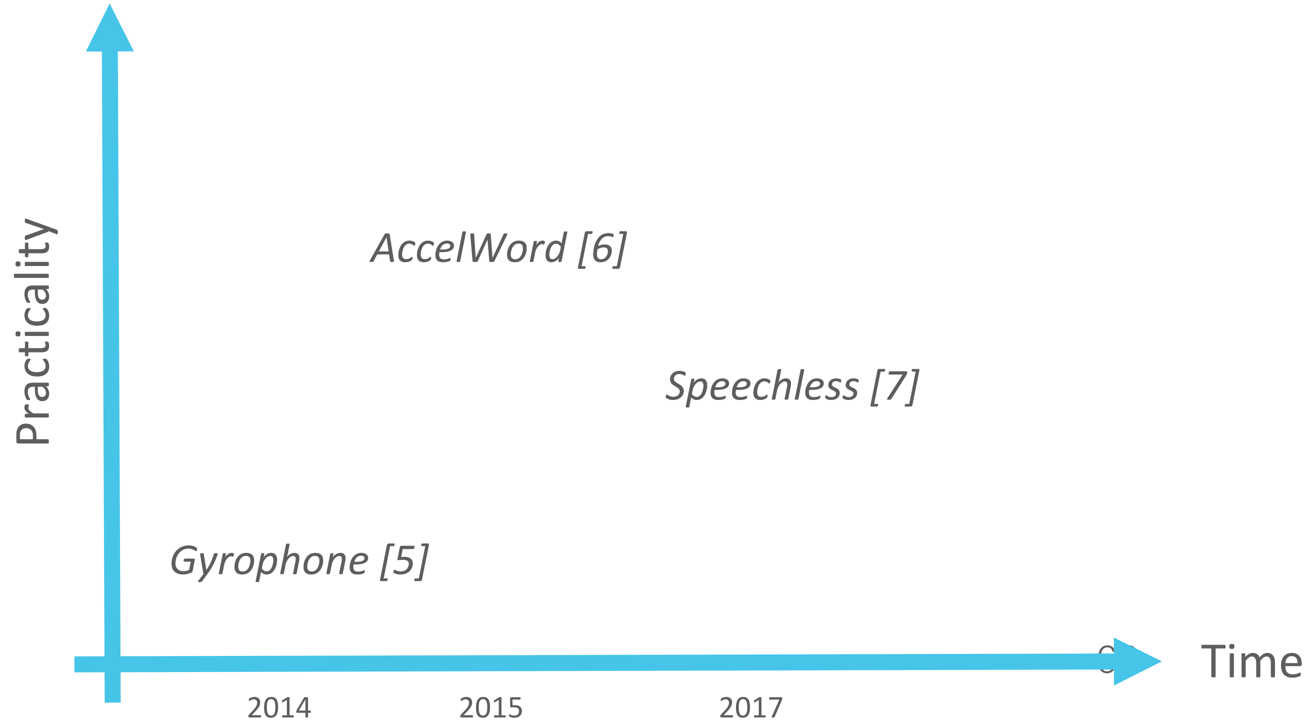
Recovering Sound from Motion Sensors

During the last seven years, the practicality of the method has improved significantly:

2015 to 2018 – Increased understanding regarding this attack vector was gained.

1st insight: MEMS accelerometers are more sensitive to acoustics than gyroscopes.

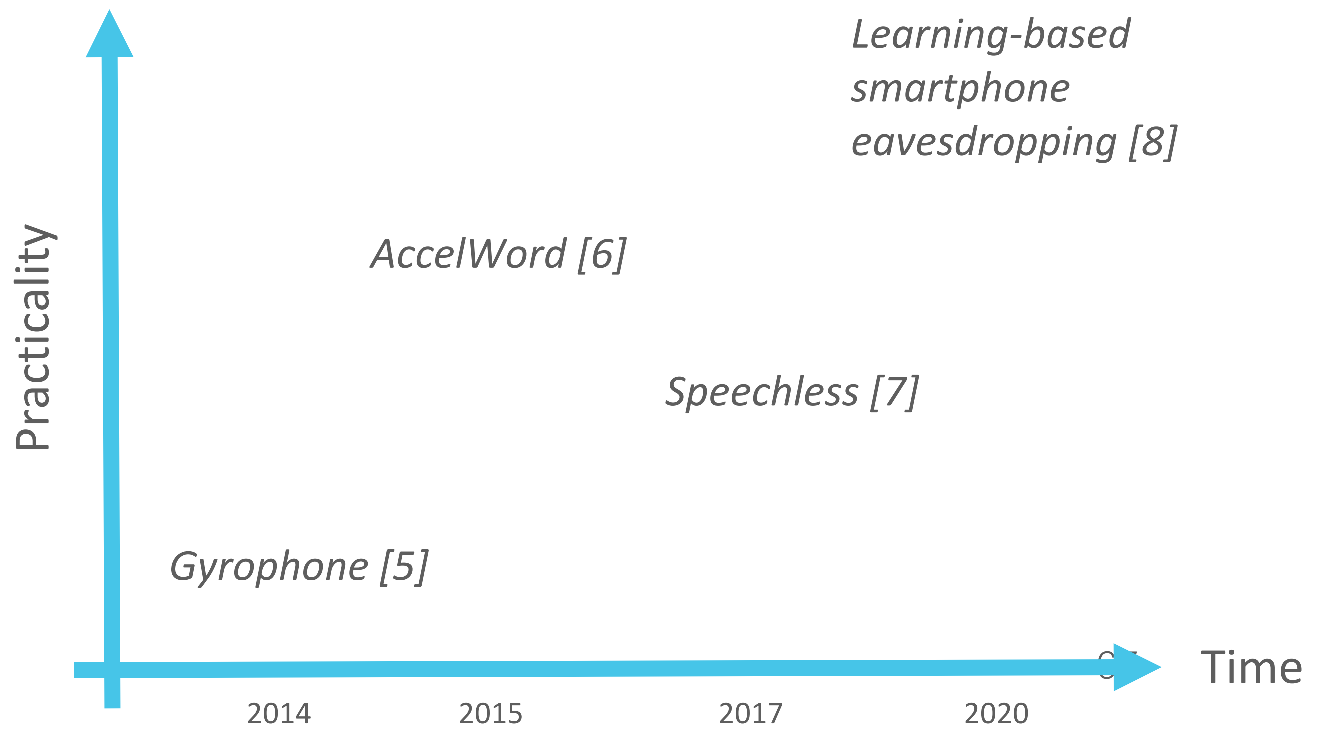
2nd insight: The effect of acoustics on motion sensors is increased when the smartphone and the speakers share the same physical surface.



Recovering Sound from Motion Sensors

During the last seven years, the practicality of the method has improved significantly:

- 2015 to 2018 – Increased understanding regarding this attack vector was gained.
- 2020 – The attack vector was improved to make it a real and practical threat to privacy.
  - Some smartphones allow a sampling rate of 500 Hz.
  - Neural networks were used to classify words instead of the KNN approach. This yields excellent accuracy.
  - The attack vector relies on speech at a normal volume.



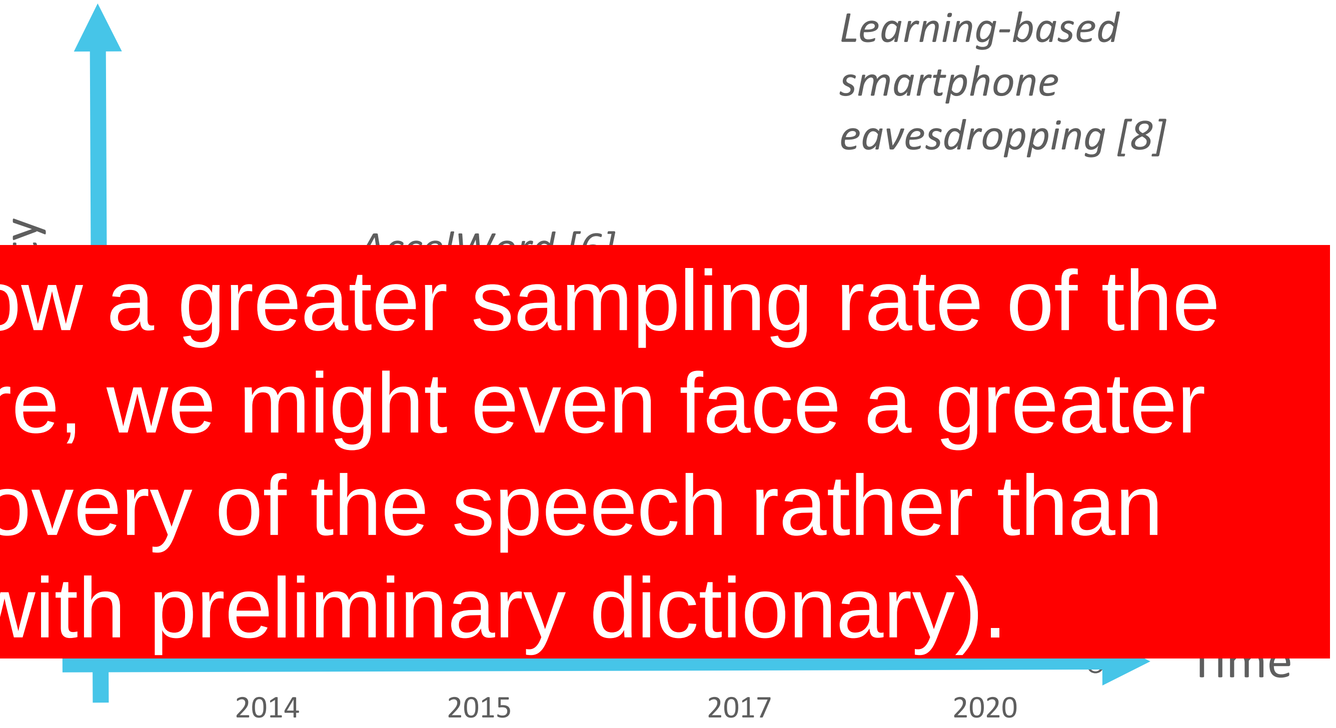
Recovering Sound from Motion Sensors

During the last seven years, the practicality of the method has improved significantly:

2015 to 2018 – Increased understanding regarding this attack vector was gained.

2020 – The attack vector was improved to make it a real and practical threat to privacy.

Some smartphones allow a sampling rate

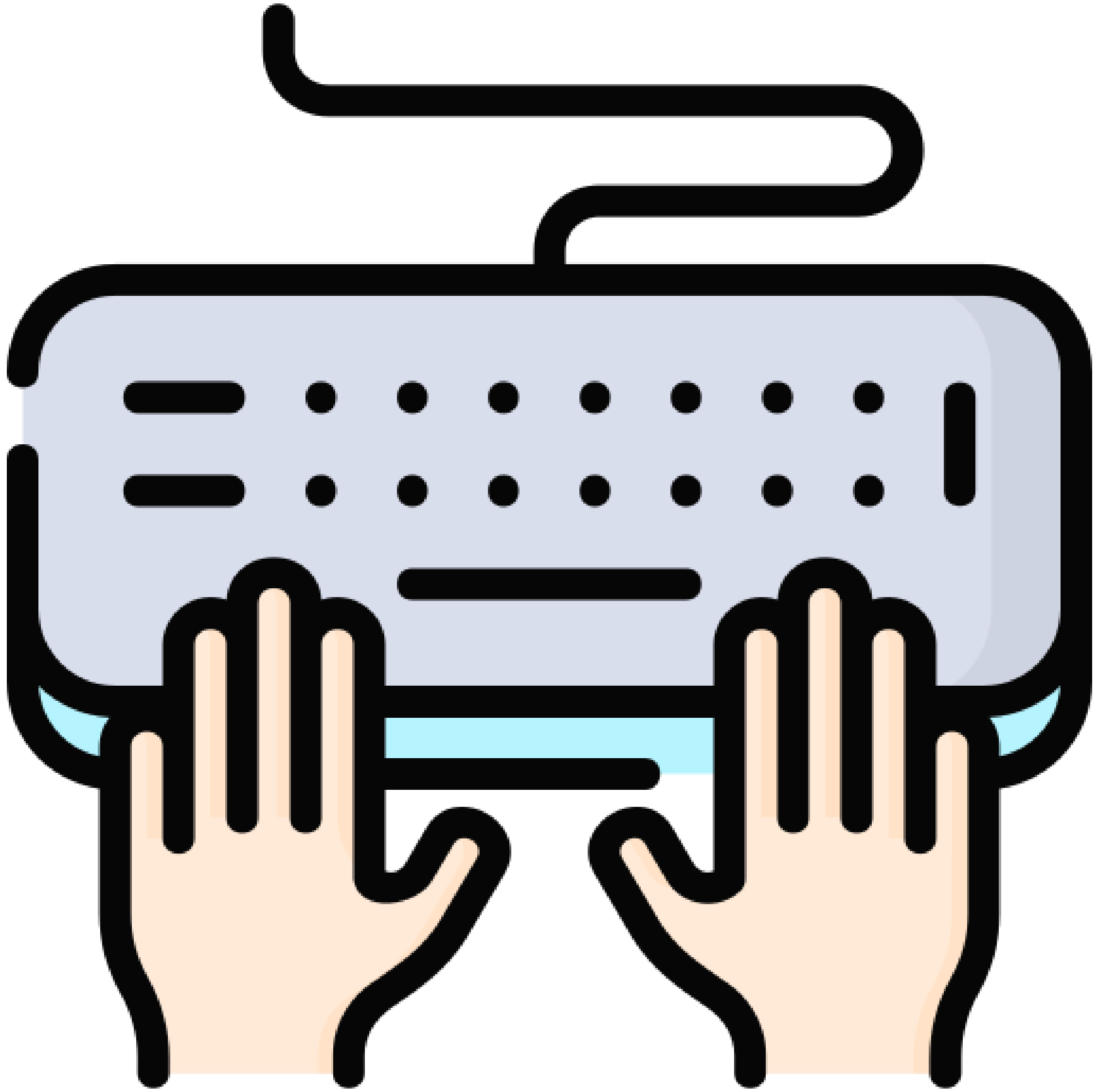


If smartphones manufacturers will allow a greater sampling rate of the integrated motion sensors in the future, we might even face a greater problem (i.e., a complete sound recovery of the speech rather than classification of isolated words with preliminary dictionary).

Recovering Sound from Motion Sensors

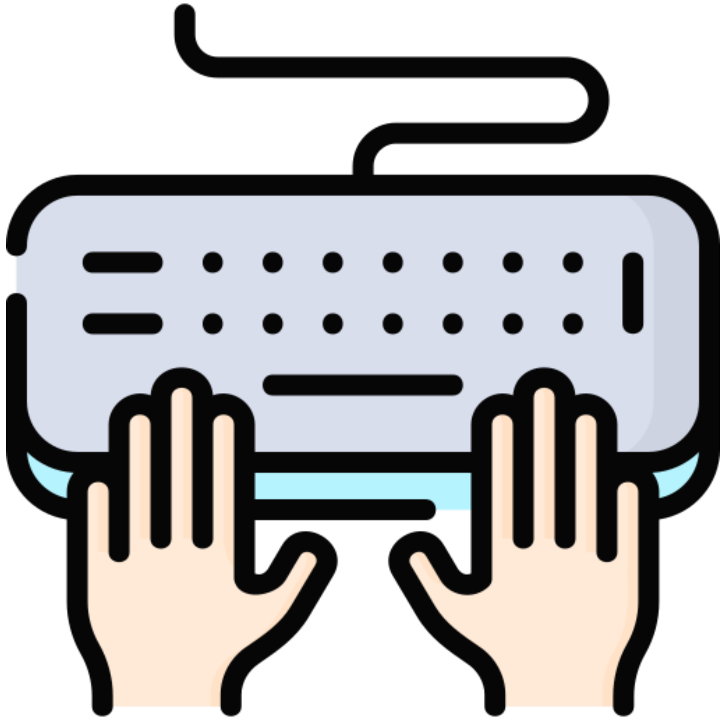
Case study 2

Question: Can motion sensors data be used for keylogging?



Keylogging

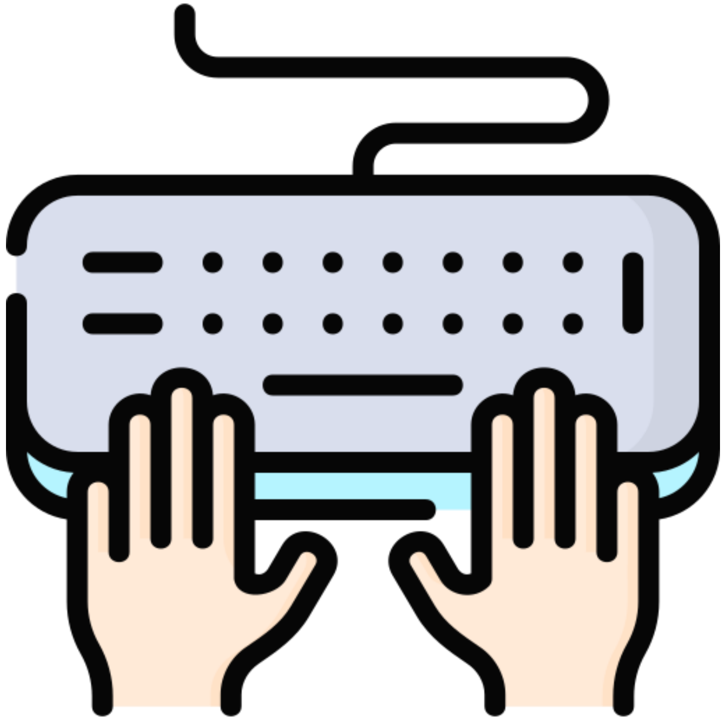
Keylogging is the process of recovering the typed text or password from data.



Keylogging

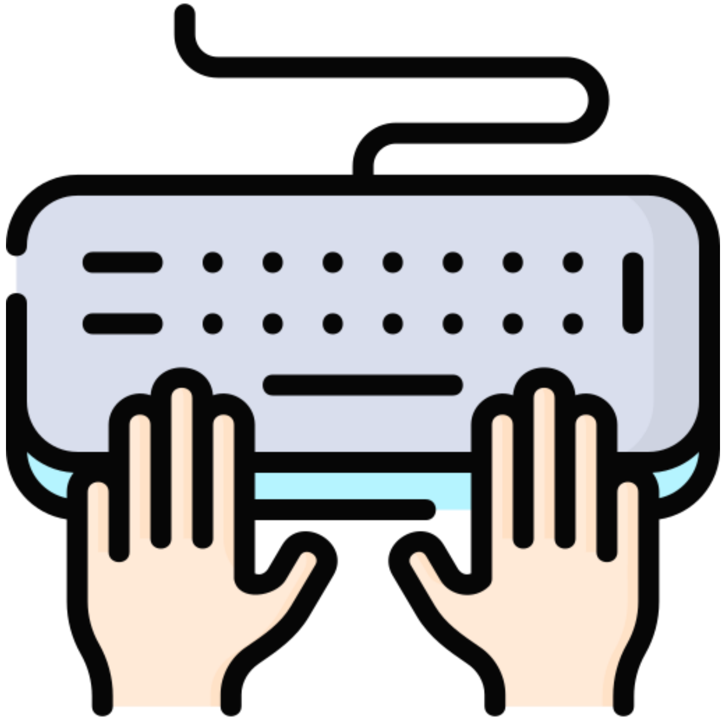
Keylogging is the process of recovering the typed text or password from data.

Various methods were already suggested to create keyloggers.



Keylogging

Keylogging is the process of recovering the typed text or password from data.



Various methods were already suggested to create keyloggers.

Keylogging is usually done by analyzing data (e.g., acoustic data obtained from microphones) influenced by the side effects of typing.

Keylogging

If a user wears a smartwatch while typing on a keyboard, we expect the data from the motion sensors to indicate the movement of the wrist on the keyboard.

Keylogging

If a user wears a smartwatch while typing on a keyboard, we expect the data from the motion sensors to indicate the movement of the wrist on the keyboard.

Attackers need to overcome a primary challenge:

- **Missing information: Assuming that the user wears the smartwatch on his/her left hand, attackers can only recover the characters on the left side of the keyboard.**

Keylogging

How can attackers fill in the missing gaps [9],[10],[11]?

Attackers can detect strokes on the left side of the keyboard by analyzing data from motion sensors.

Keylogging

How can attackers fill in the missing gaps [9],[10],[11]?

Attackers can detect strokes on the left side of the keyboard by analyzing data from motion sensors.

Attackers can identify missing strokes on the right side of the keyboard by analyzing the motion sensor signal in the time domain to identify gaps and infer the number of missing characters.

Keylogging

How can attackers fill in the missing gaps [9],[10],[11]?

Attackers can detect strokes on the left side of the keyboard by analyzing data from motion sensors

Attackers can identify missing strokes on the right side of the keyboard by analyzing the motion sensor signal in the time domain to identify gaps and infer the number of missing characters.

Attackers can use a statistical model to fill in the missing characters using a dictionary.

Keylogging

How can attackers fill in the missing gaps [9],[10],[11]?

Attackers can detect strokes on the left side of the keyboard by analyzing data from motion sensors.

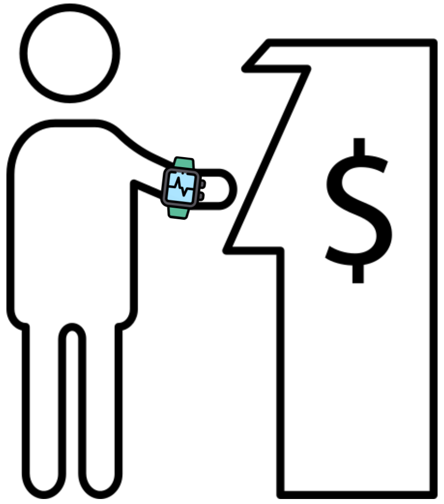
Attackers can identify strokes on the right side

This approach was implemented in various studies [9-11], showing good accuracy in recovering typing.

Keylogging

Conclusions:

- Keylogging of the QWERTY keyboard via a smatwatch’s motion sensors is quite practical.
- The same approach can be used to recover text typed on a smartphone’s touch screen keyboard.
- Keylogging of PIN codes via a smatwatch’s motion sensors is only possible if the user uses the hand with the smartwatch to press the buttons.



Recovering Sound from Motion Sensors

Case study 3

Question: Can motion sensors data be used to detect whether an individual was intoxicated?

Detecting Intoxication

The risk to individual’s privacy:

Primary: In some Muslim countries around the world intoxication is prohibited by law, and governments penalize citizens for violating this law.

Secondary: This approach can be used to learn about another individual’s habits (e.g., by parents or bosses).

Detecting Intoxication

Question: Assuming that a party was able to obtain an individual's motion sensor data, can the data be used by that party to determine whether the individual was intoxicated or not?

Detecting Intoxication

Police officers are trained to identify an intoxicated individual based on their gait (walk and turn test).

Detecting Intoxication

Police officers are trained to identify an intoxicated individual based on their gait (walk and turn test).

This sobriety test has been used by police officers many years.

Detecting Intoxication

Police officers are trained to identify an intoxicated individual based on their gait (walk and turn test).

This sobriety test has been used by police officers for many years.

Question: Can we identify whether a person is intoxicated by analyzing motion sensor data obtained from an individual's smartphone and smartwatch during free gait?

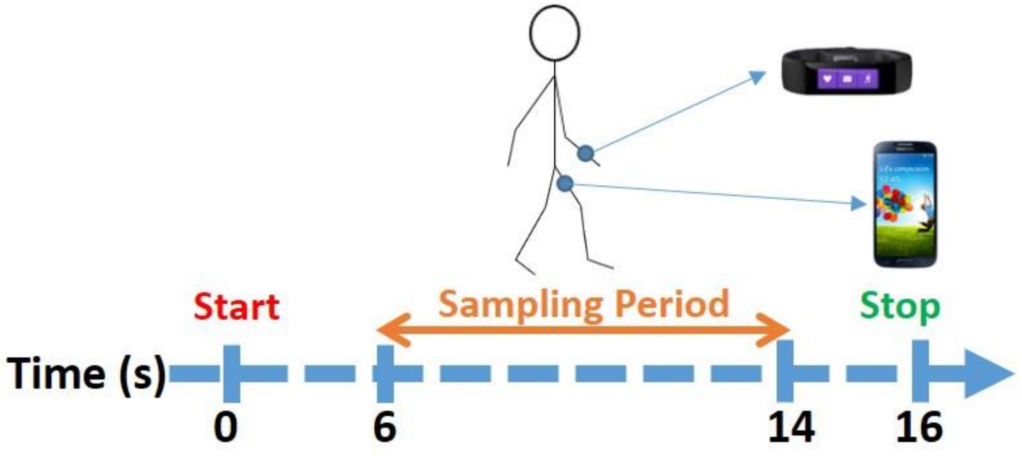
Detecting Intoxication

We performed a case study in order to answer this question, and the findings are described in the following paper:

“The Age of Testifying Wearable Devices: The Case of Intoxication Detection” [12]

Ben Nassi, Prof. Lior Rokach, and Prof. Yuval Elovici.

Detecting Intoxication



<u>The experiment</u>:

The experiment took place at three different bars

Thirty individuals participated in the experiment.

Each individual was asked to walk twice with a smartwatch and smartphone for 16 seconds (only eight seconds of the motion sensor data was used):

The first walk took place before the individual started to drink

The second walk took place after the individual completed to drink.

The second time, we measured the breath alcohol concentration of each of the participants with a professional breathalyzer.

Detecting Intoxication

Feature Engineering:

For each individual, we extracted two feature vectors:

Detecting Intoxication

Feature Engineering:

For each individual, we extracted two feature vectors:

- **One vector was extracted from the data obtained before the individual started to drink.**

Detecting Intoxication

Feature Engineering:

For each individual, we extracted two feature vectors:

One vector was extracted from the data obtained before the individual started to drink.

The second vector was extracted from the data obtained after the individual completed to drink.

Detecting Intoxication

Feature Engineering:

For each individual, we extracted two feature vectors:

- One vector was extracted from the data obtained before the individual started to drink.
- The second vector was extracted from the data obtained after the individual completed to drink.
- **The vectors consist of the exact same features: (a) statistical features, (b) distribution in the time domain, (c) distribution in the frequency domain, and (d) known gait features.**

Detecting Intoxication

Feature Engineering:

For each individual:

We subtracted the values of the second vector from the first vector and created a vector of differences.

Detecting Intoxication

Feature Engineering:

For each individual:

We subtracted the values of the second vector from the first vector and created a vector of differences.

We labeled the vector of differences with the breath alcohol concentration sample that was taken from the breathalyzer.

Detecting Intoxication

Feature Engineering:

For each individual:

- We subtracted the values of the second vector from the first vector and created a vector of differences.
- We labeled the vector of differences with the breath alcohol concentration sample that was taken from the breathalyzer.

We ended up with 30 vectors (one for each participant) that indicate the difference in a person's free gait labeled by their breath alcohol concentration level.

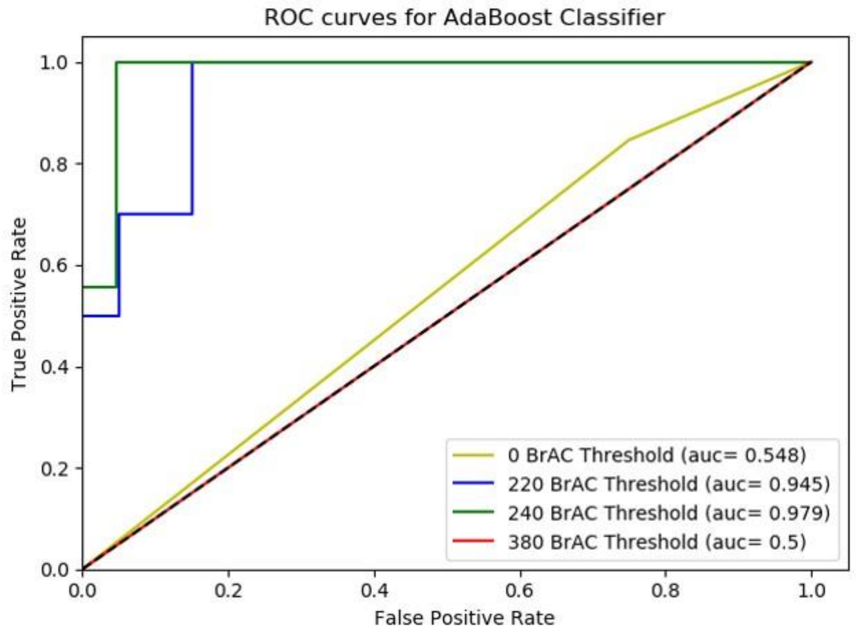
Detecting Intoxication

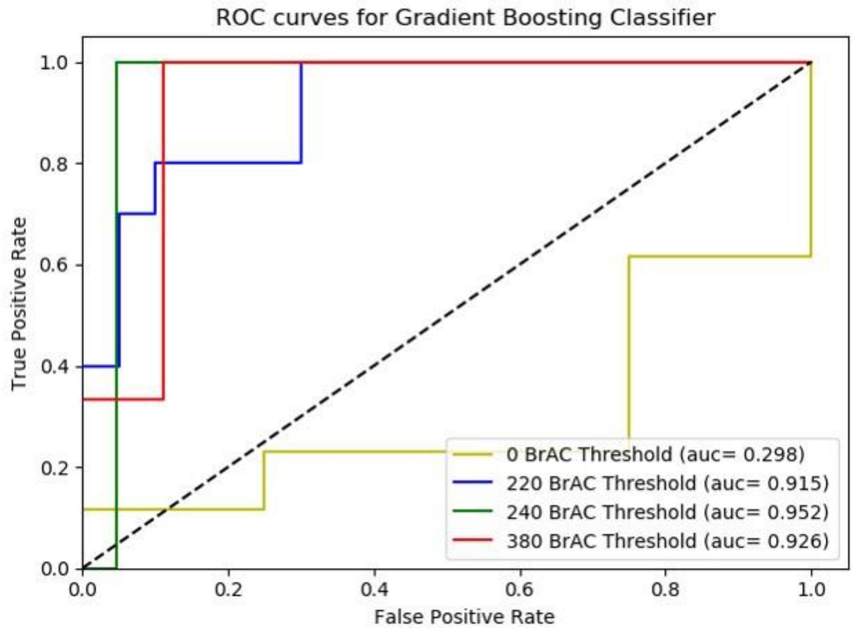
Results

We examined whether an individual's intoxication level can be determined for various BrAC levels (0, 220, 240, 380).

We compared the results of two ML algorithms: Gradient Boosting Classifier and AdaBoost classifier.

We found that our models can identify intoxicated individuals with a BrAC > 220 with a AUC > 0.91.





Detecting Intoxication

Results

The models are not perfect.

They each have FP and FN detections.

In some cases we cannot tolerate a specific type of mistake, and we want to evaluate the model's performance with respect to various policies.

	Predicted							
	0		**220**		**240**		**380**	
	Drunk	Sober	Drunk	Sober	Drunk	Sober	Drunk	Sober
Drunk	1	3	8	2	9	0	0	3
Sober	4	22	3	17	1	20	0	27

Table 3: Confusion matrices of the AdaBoost for BrAC thresholds of 0, 220, 240, and 380.

	Predicted							
	0		**220**		**240**		**380**	
	Drunk	Sober	Drunk	Sober	Drunk	Sober	Drunk	Sober
Drunk	1	3	6	4	9	0	0	3
Sober	4	22	1	19	2	19	0	27

Table 2: Confusion matrices of the Gradient Boosting Classifier for BrAC thresholds of 0, 220, 240, and 380.

Detecting Intoxication

Is it possible to tune the model to detect all intoxicated subjects?

This can be accomplished by:

Setting the model's TPR at 1.0 and analyzing how this affects the FPR, considering, e.g., how many sober individuals are misdetected as a result.

In general, we found that the FPR remains very low.

	Thresholds			
	0	**220**	**240**	**380**
GBC	1	0.3	0.09	0.11
AdaBoost	1	0.15	0.04	0

Table 4: Detecting all intoxicated subjects: FPR (false positive rate) of classifiers with a fixed TPR (true positive rate) of 1.0.

Detecting Intoxication

Is it possible to tune the model so that all individuals detected as intoxicated by the model are actually intoxicated?

This can be accomplished by:

Setting the model's FPR at 0 and analyzing how this affects the TPR, considering, e.g., how many intoxicated individuals are missed as a result.

In general, this policy can result in many errors.

	Thresholds			
	0	**220**	**240**	**380**
GBC	0	0.4	0	0
AdaBoost	0	0.4	0.55	0

Table 5: Detecting an intoxicated instance with no errors: TPR (true positive rate) of classifiers with a fixed FPR (false positive rate) of zero.

Takeaways

Takeaways

The primary risk that motion sensors currently pose is to individuals' privacy (rather than posing a threat to device security).

Takeaways

The primary risk that motion sensors currently pose is to individuals’ privacy (rather than posing a threat to device security).

Many people don’t consider data from motion sensors a privacy risk, however attackers can derive various insights about users by analyzing motion sensor data:

- **Recovering speech**
- **Keylogging**
- **Detect whether an individual is intoxicated**
- **Alternative way to locate a user (instead of GPS)**
- **User identification**

Takeaways

The primary risk that motion sensors currently pose is to individuals' privacy (rather than posing a threat to device security).

Many people don't consider data from motion sensors a privacy risk, however attackers can derive various insights about users by analyzing motion sensor data.

Currently, the most practical way to obtain motion sensor data requires the attacker to install an application on an IoT device in order to obtain motion sensor data.

Takeaways

The primary risk that motion sensors currently pose is to individuals' privacy (rather than posing a threat to device security).

Many people don't consider data from motion sensors a privacy risk, however attackers can derive various insights about users by analyzing motion sensor data.

Currently, the most practical way to obtain motion sensor data requires the attacker to install an application on an IoT device in order to obtain motion sensor data.

However, we expect that ongoing external changes (adoption of 5G, increased commercial interest in motion sensor data) will result in increased data collection by third parties. As a result, we believe that in the near future, obtaining motion sensor data via third parties will become more practical than installing a malicious application.

Takeaways

The primary risk that motion sensors currently pose is to individuals' privacy (rather than posing a threat to device security).

Many people don't consider data from motion sensors a privacy risk, however attackers can derive various insights about users by analyzing motion sensor data.

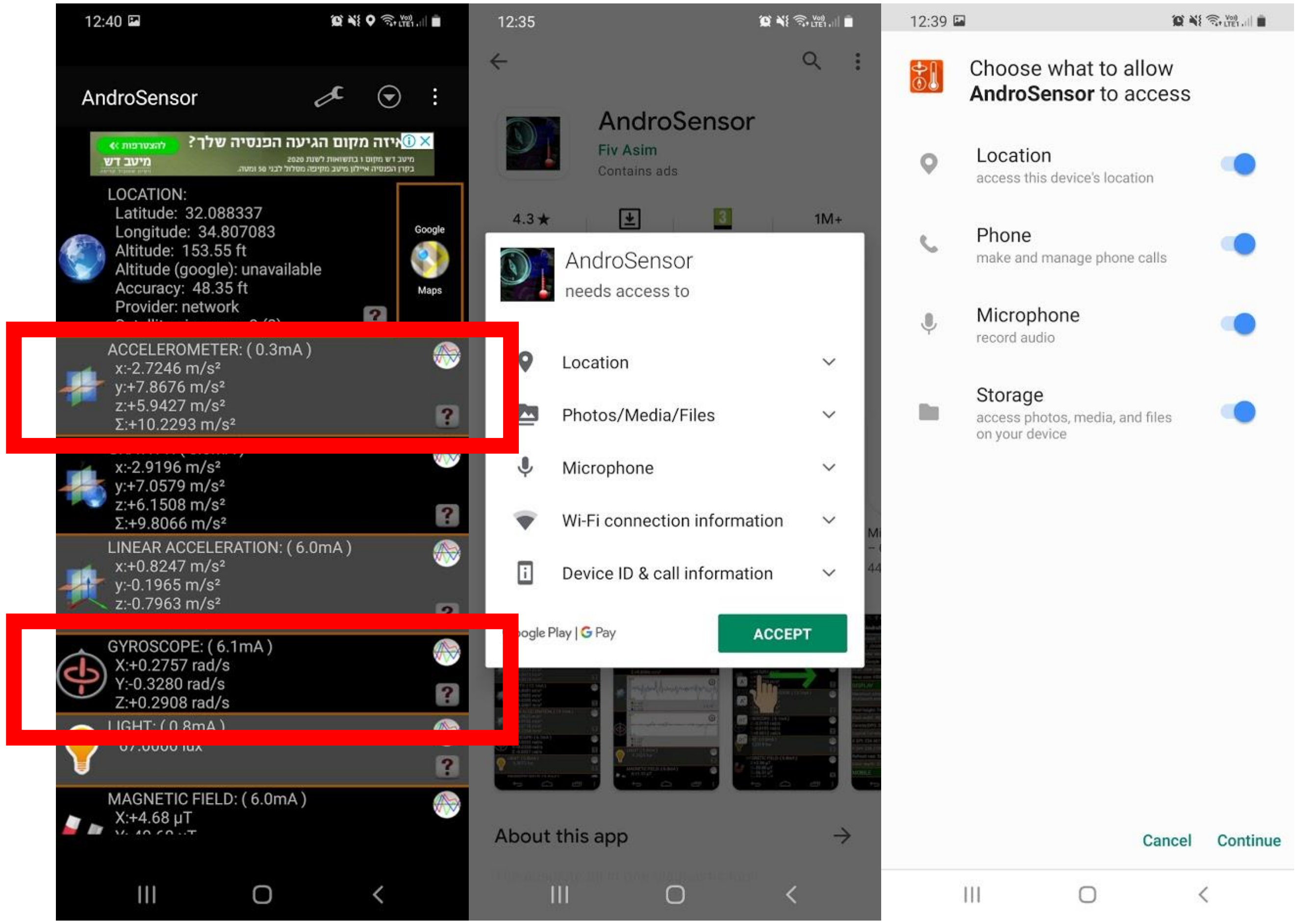
Currently, the most practical way to obtain motion sensor data requires the attacker to install an application on an IoT device in order to obtain motion sensor data.

However, we expect that ongoing external changes (adoption of 5G, increased commercial [illegible] become more practical than installing a malicious application.

We believe that the common threat model to obtain motion sensor data is about to be change in the near future due to external changes.

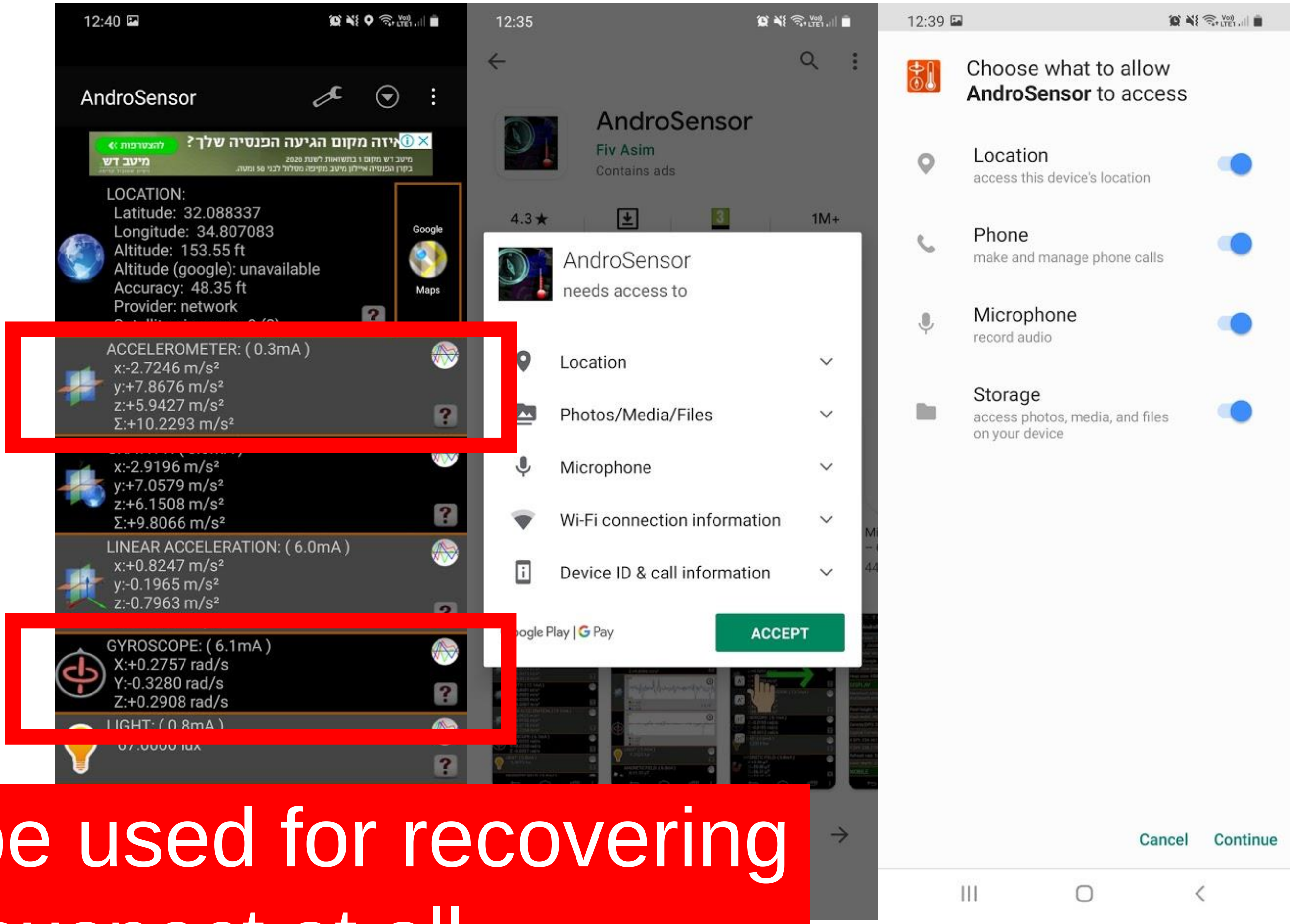
Takeaways

Considering our understanding about the privacy risks associated with motion sensor data, we are quite surprised that such data can be obtained without user permission.



Takeaways

Considering our understanding about the privacy risks associated with motion sensor data, we are quite surprised that such data can be obtained without user permission.



A user’s motion sensor data might be used for recovering speech and the user won’t suspect at all.

Takeaways

Last point to think about:

Throughout the entire talk, we considered the fact that deriving insights about a user by analyzing the collected motion sensor data is a violation of the user’s privacy.

This is true from a user perspective.

What about the bigger picture?

Takeaways

In a few well-known cases, a user's motion sensor data was used to:

Takeaways

In a few well-known cases, a user’s motion sensor data was used to:

Contradict a husband’s report of his wife’s time of death, which changed the course of the investigation by enabling the police to prove that she was walking around an hour after her husband told the police she was shot by an invader.

A Fitbit Helped Police Arrest A Man For His Wife's Murder

The fitness tracker recorded the woman moving around her house for an hour after her husband told police she was shot by a home invader.

Mary Ann Georgantopoulos
BuzzFeed News Reporter

Takeaways

In a few well-known cases, a user's motion sensor data was used to:

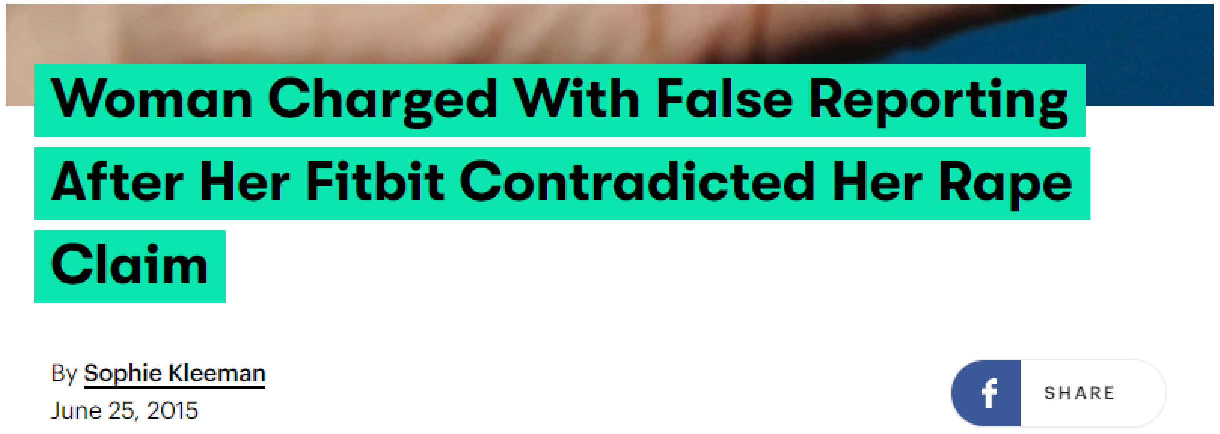
Contradict a husband's report of his wife's time of death, which changed the course of the investigation by enabling the police to prove that she was walking around an hour after her husband told the police she was shot by an invader.

Charge a woman with false reporting after her Fitbit contradicted her rape claim by proving that she was actually walking around at the time in question.

A Fitbit Helped Police Arrest A Man For His Wife's Murder

The fitness tracker recorded the woman moving around her house for an hour after her husband told police she was shot by a home invader.

Mary Ann Georgantopoulos
BuzzFeed News Reporter



Woman Charged With False Reporting After Her Fitbit Contradicted Her Rape Claim

By Sophie Kleeman
June 25, 2015

SHARE

Takeaways

In a few well-known cases, a user's motion sensor data was used to:

Co

de

by

arc

wa

Ch

co

actually walking around at the time in question.

The answer to the question of whether we want to allow a party to analyze an individual's motion sensor data, depends on the usecase.

In some usecases, this can help the police to solve crimes.

e Arrest A
Murder

und her house for an hour after her
r.

alse Reporting
cted Her Rape

By Sophie Kleeman
June 25, 2015

SHARE

Thank You

Questions

Bibliography

[1] CASTRO, S., DEAN, R., ROTH, G., FLOWERS, G. T., AND GRANTHAM, B. Influence of acoustic noise on the dynamic performance of MEMS gyroscopes. In International Mechanical Engineering Congress and Exposition (2007), American Society of Mechanical Engineers

[2] DEAN, R. N., FLOWERS, G. T., HODEL, A. S., ROTH, G., CASTRO, S., ZHOU, R., MOREIRA, A., AHMED, A., RIFKI, R., GRANTHAM, B. E., ET AL. On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise. In IEEE International Symposium on Industrial Electronics (2007).

[3] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., ... & Kim, Y. (2015). Rocking drones with intentional sound noise on gyroscopic sensors. In 24th {USENIX} Security Symposium ({USENIX} Security 15) (pp. 881-896).

[4] Trippel, T., Weisse, O., Xu, W., Honeyman, P., & Fu, K. (2017, April). WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In 2017 IEEE European symposium on security and privacy (EuroS&P) (pp. 3-18). IEEE.

Bibliography

[5] Y. Michalevsky, D. Boneh, and G. Nakibly, “Gyrophone: Recognizing speech from gyroscope signals,” in 23rd USENIX Security Symposium (USENIX Security 14). San Diego, CA: USENIX Association, 2014, pp. 1053–1067.

[6] L. Zhang, P. H. Pathak, M. Wu, Y. Zhao, and P. Mohapatra, “Accelword: Energy efficient hotword detection through accelerometer,” in Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services. ACM, 2015, pp. 301–315.

[7] S. A. Anand and N. Saxena, “Speechless: Analyzing the threat to speech privacy from smartphone motion sensors,” in 2018 IEEE Symposium on Security and Privacy (SP), vol. 00, pp. 116–133.

[8] Z. Ba, T. Zheng, X. Zhang, Z. Qin, B. Li, X. Liu, and K. Ren, “Learning-based practical smartphone eavesdropping with built-in accelerometer.” Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2020.

Bibliography

[9] H. Wang, T. T.-T. Lai, and R. Roy Choudhury, “Mole: Motion leaks through smartwatch sensors,” in Proceedings of the 21st Annual International Conference on Mobile Computing and Networking. ACM, 2015, pp. 155–166.

[10] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang, “When good becomes evil: Keystroke inference with smartwatch,” in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 1273–1285.

[11] L. Cai and H. Chen, “On the practicality of motion based keystroke inference attack,” in International Conference on Trust and Trustworthy Computing. Springer, 2012, pp. 273–290.

[12] Nassi, Ben, Lior Rokach, and Yuval Elovici. "The Age of Testifying Wearable Devices: The Case of Intoxication Detection.