

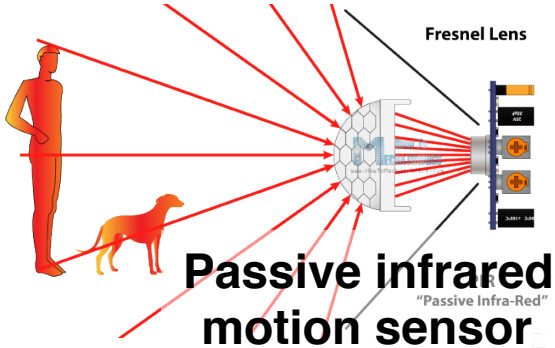
Hacking Sensors

Yongdae Kim

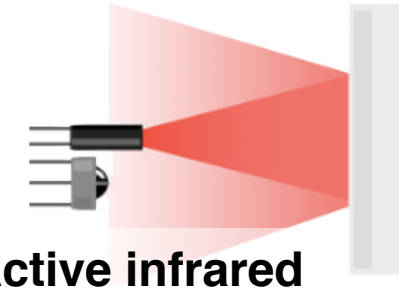
SysSec@KAIST

Sensor

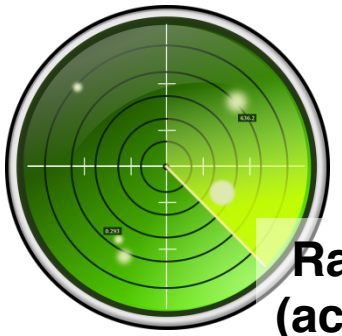
- Sensor = An electrical device
  - To measure physical properties of surrounding environment
  - Passive and active sensors



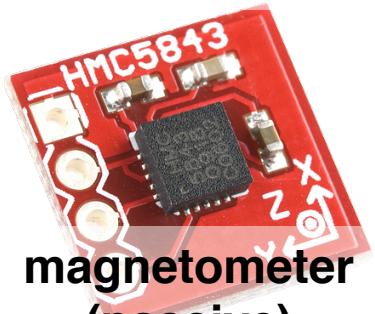
Passive infrared motion sensor



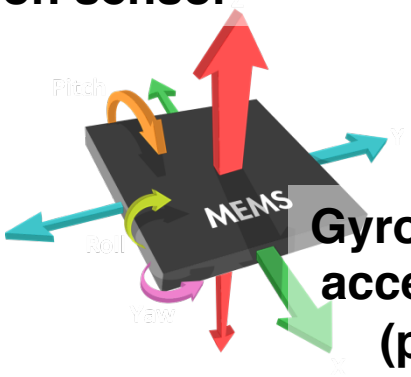
Active infrared range sensor



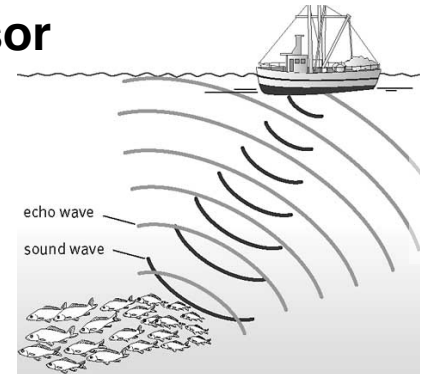
Radar (active)



magnetometer (passive)



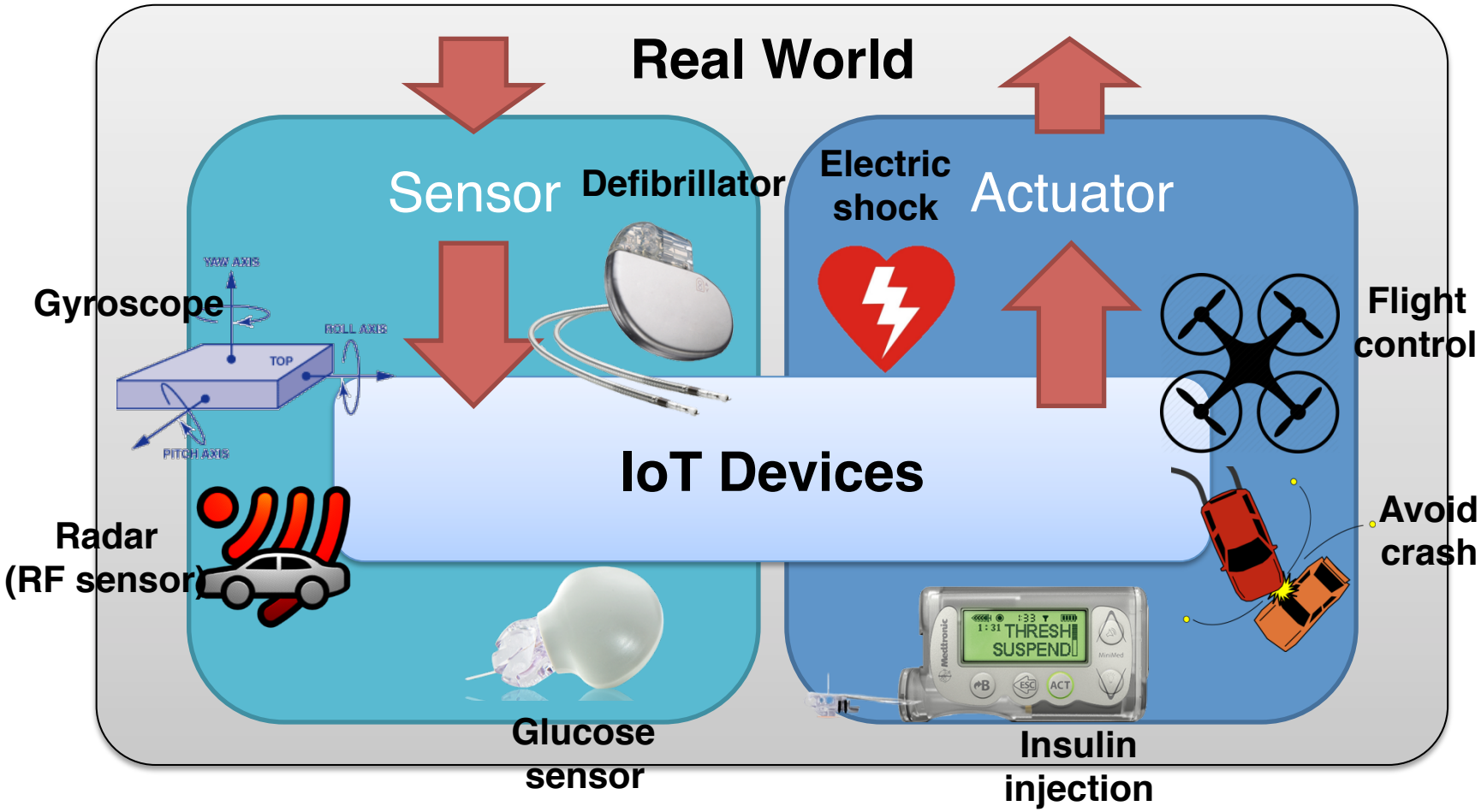
Gyroscope and accelerometer (passive)



Sonar (active)

Sensing & Actuation

- Actuation and decision-making based on sensor data



TOP MARKET CAP INCREASES

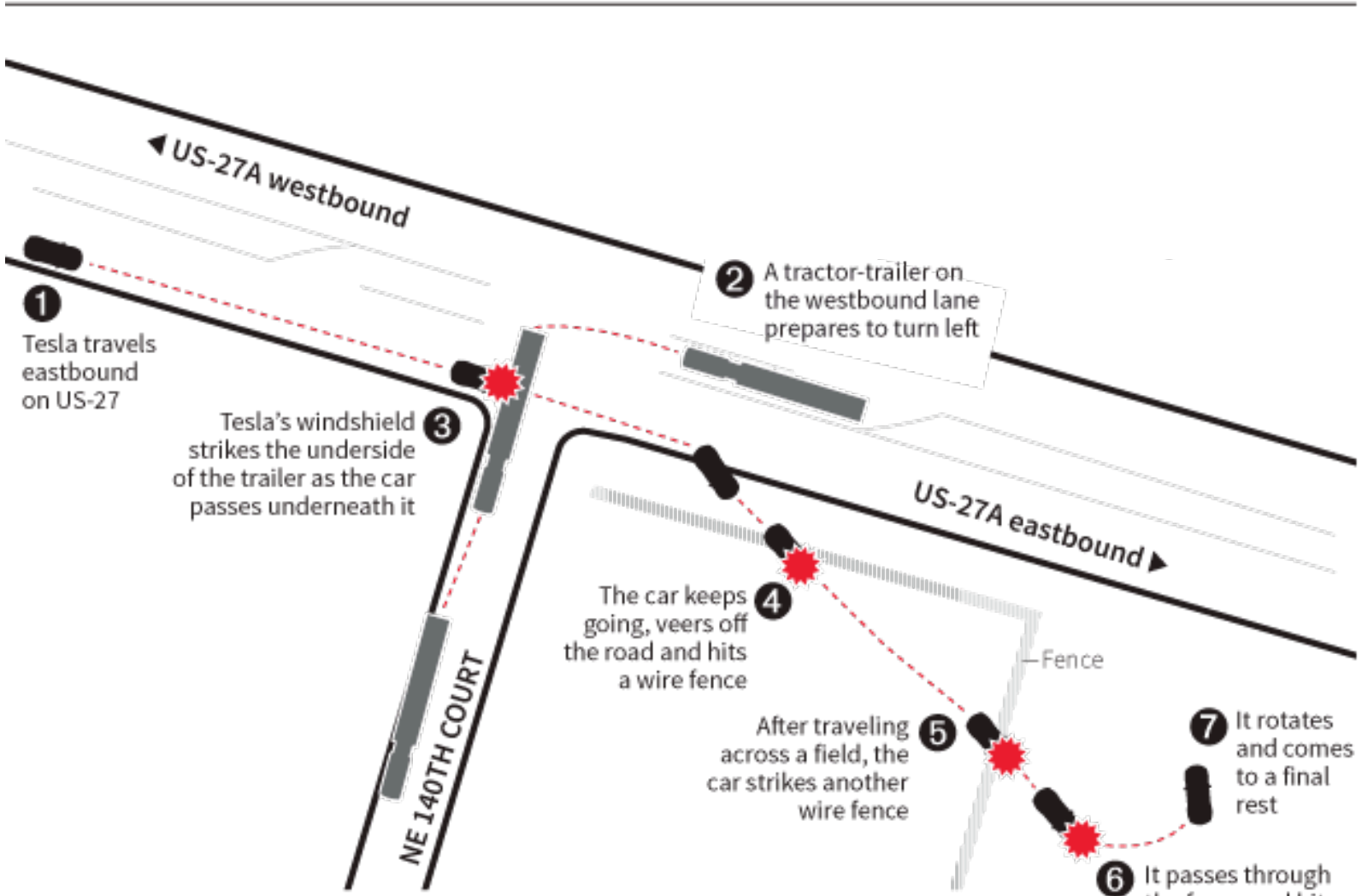


Diagram not to scale.

Sources: Florida Highway Patrol Troop; U.S. National Highway Traffic Safety Administration

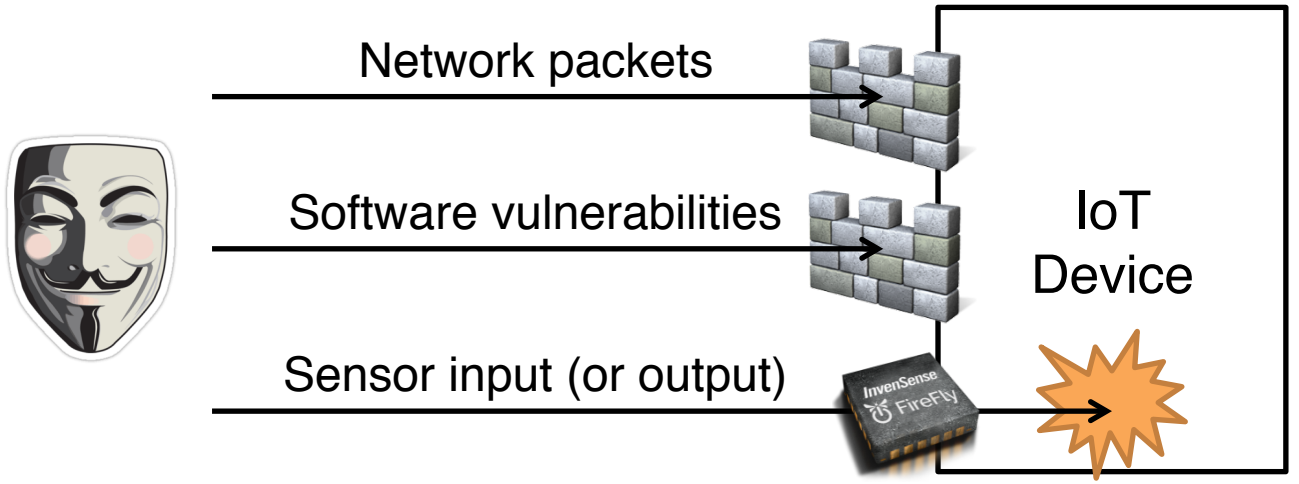
C. Chan, 30/06/2016

REUTERS

Sensor & Security

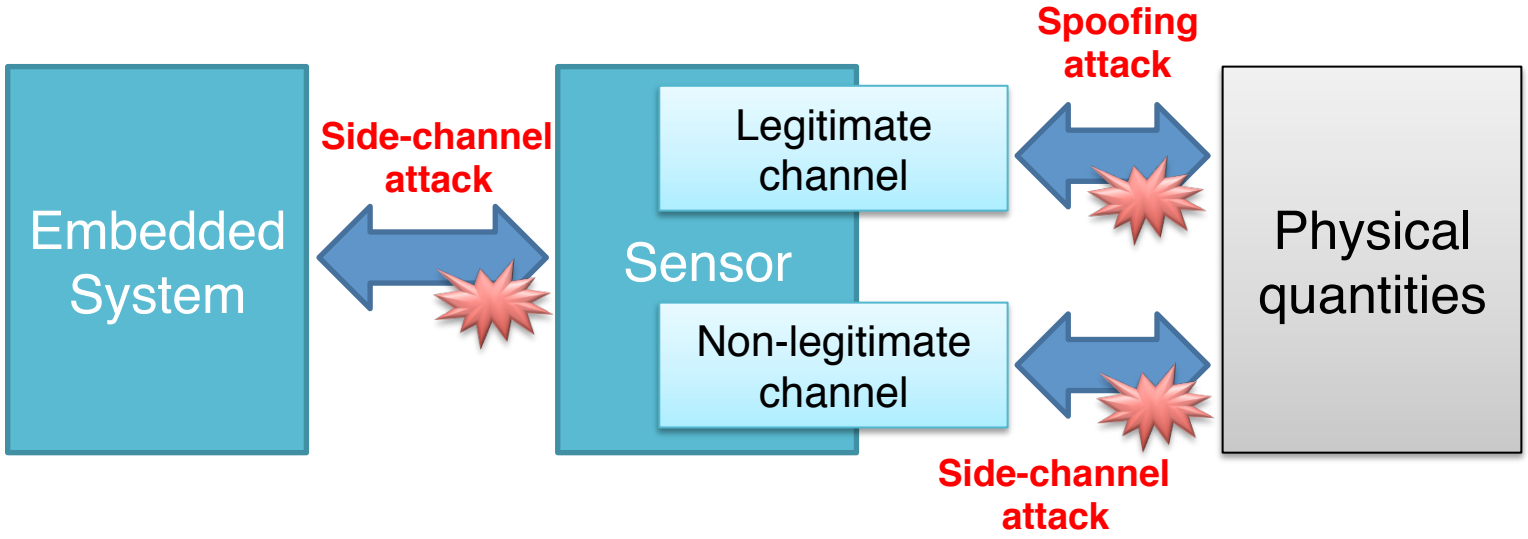
- Many prevention and detection mechanisms
  - For malicious network traffics
  - For software vulnerabilities

Sensor = A new attack vector

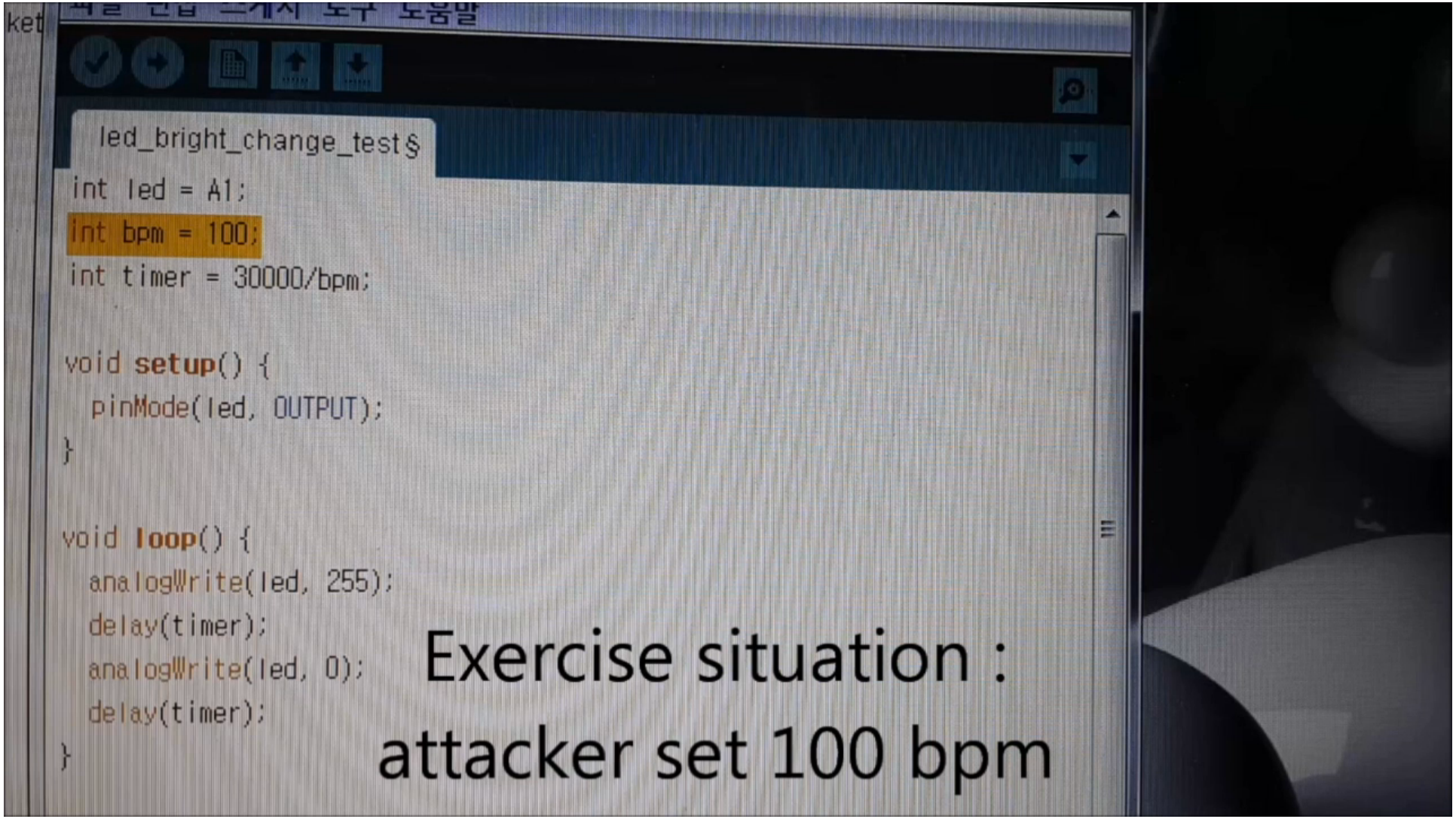


Attack Vectors of Sensors

- Three interfaces
  - Sensitive to legitimate physical quantities
  - Insensitive to other physical quantities
  - Need to send sensor data to the system

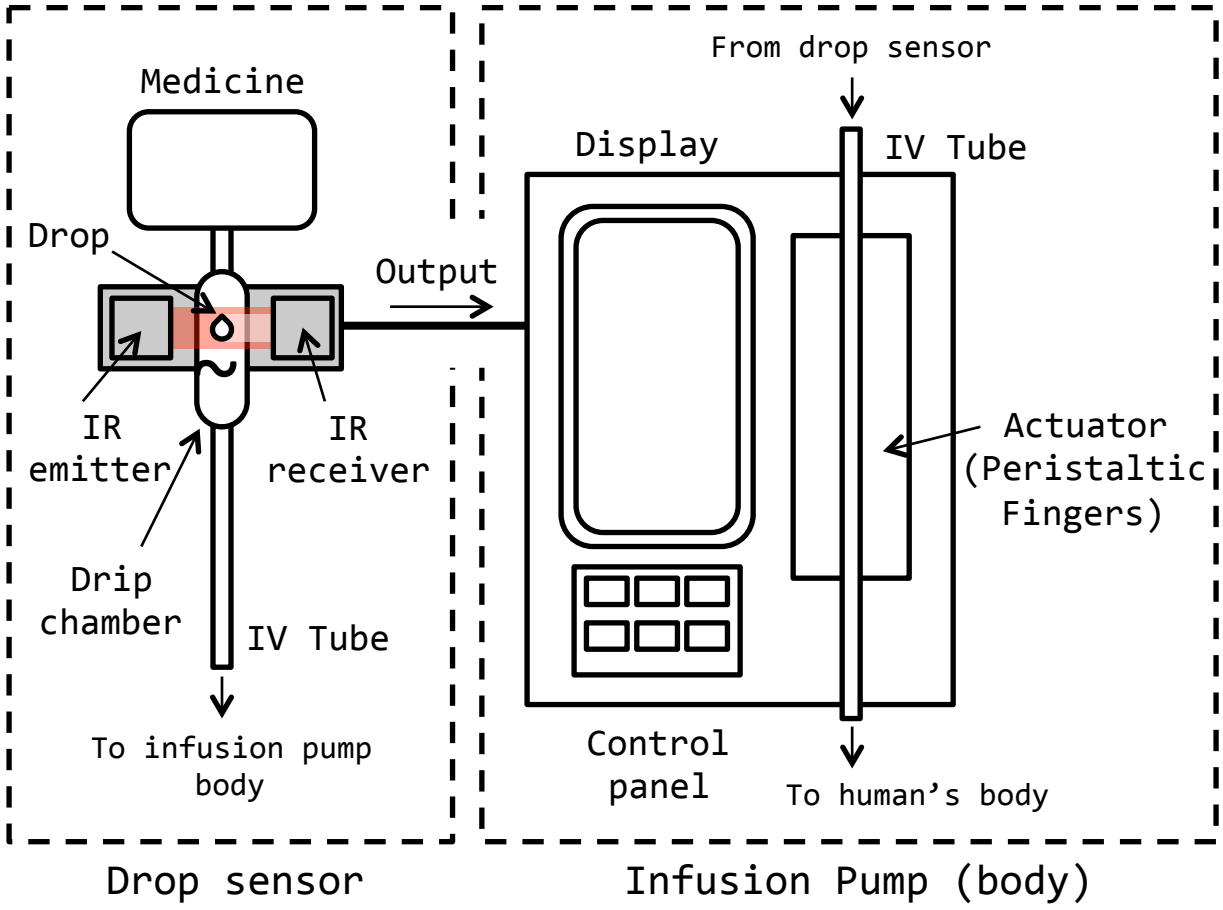


Heart Rate Sensor Spoofing



Target: Medical Infusion Pump

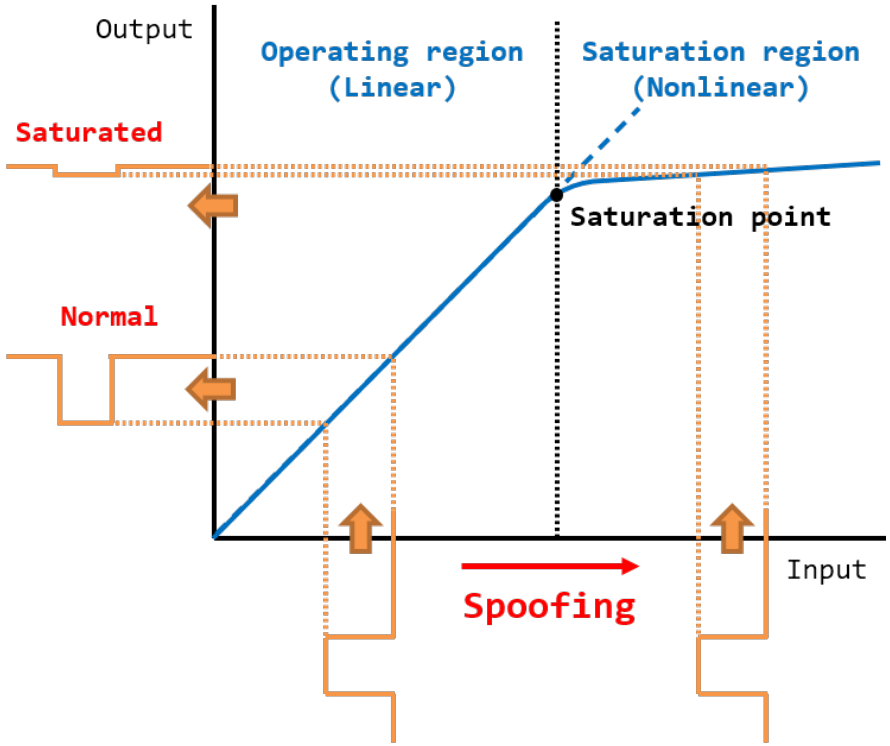
- Controlling infused volume of medicine to patients
- Sometimes using a drop sensor for accuracy



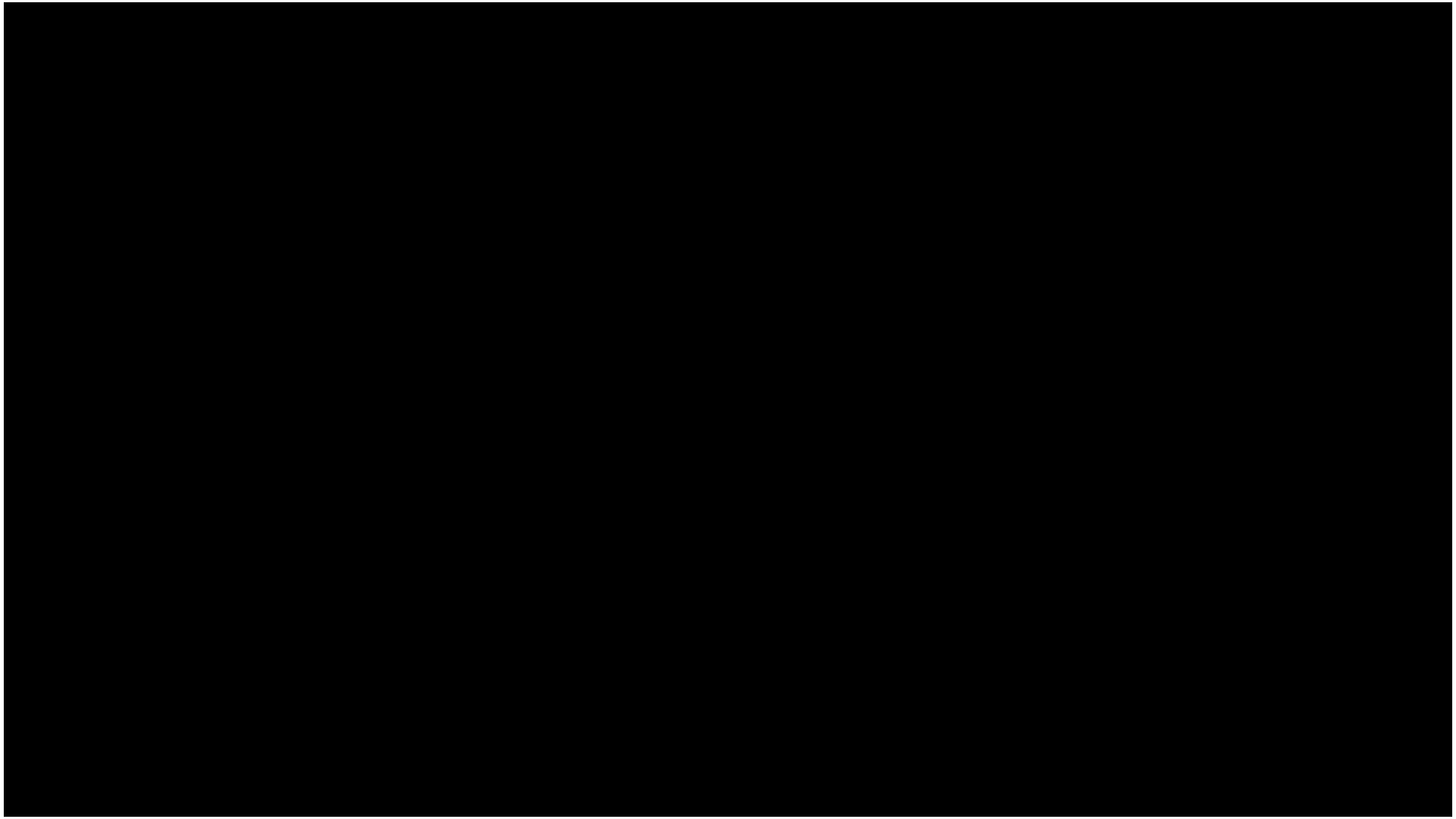
Park et.al, This ain't your dose: Sensor Spoofing Attack on Medical Infusion Pump, Usenix WOOT'16

Sensor Saturation

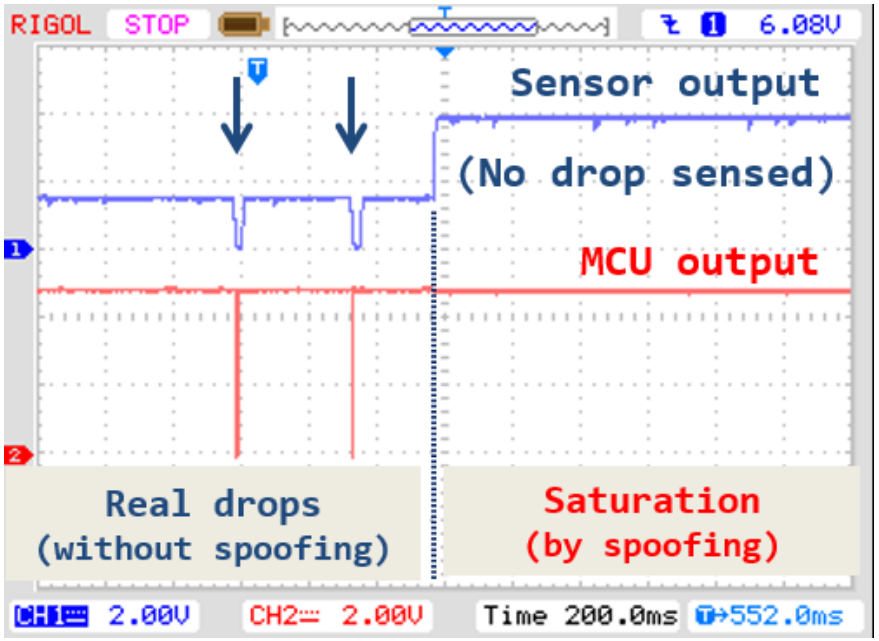
- New type of sensor spoofing attack using **saturation**
  - Sensors have typical operating region
  - Output is saturated when exceeding a saturation point
  - Possible to sensors using non-countervailed source (e.g. light)

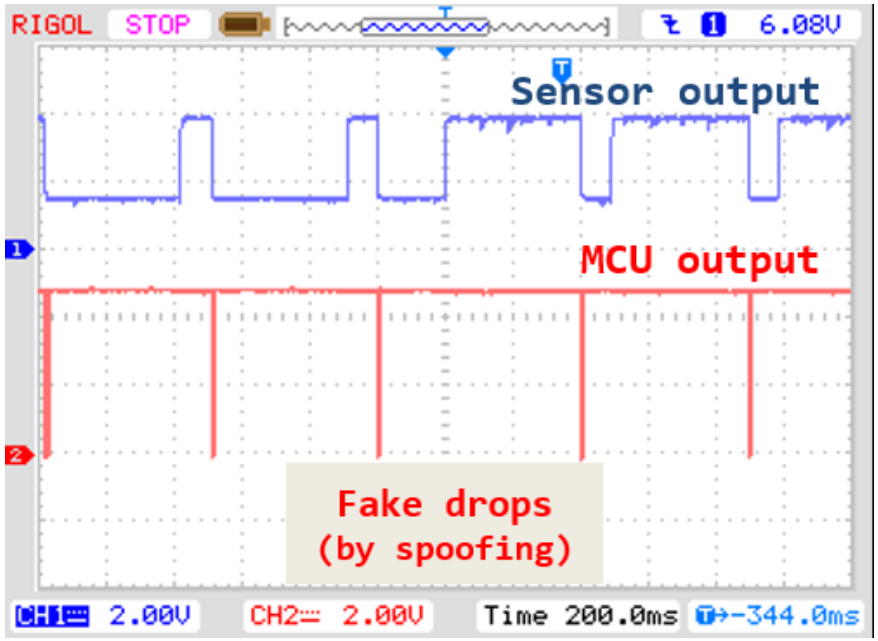


Infusion Pump and Drop Sensor

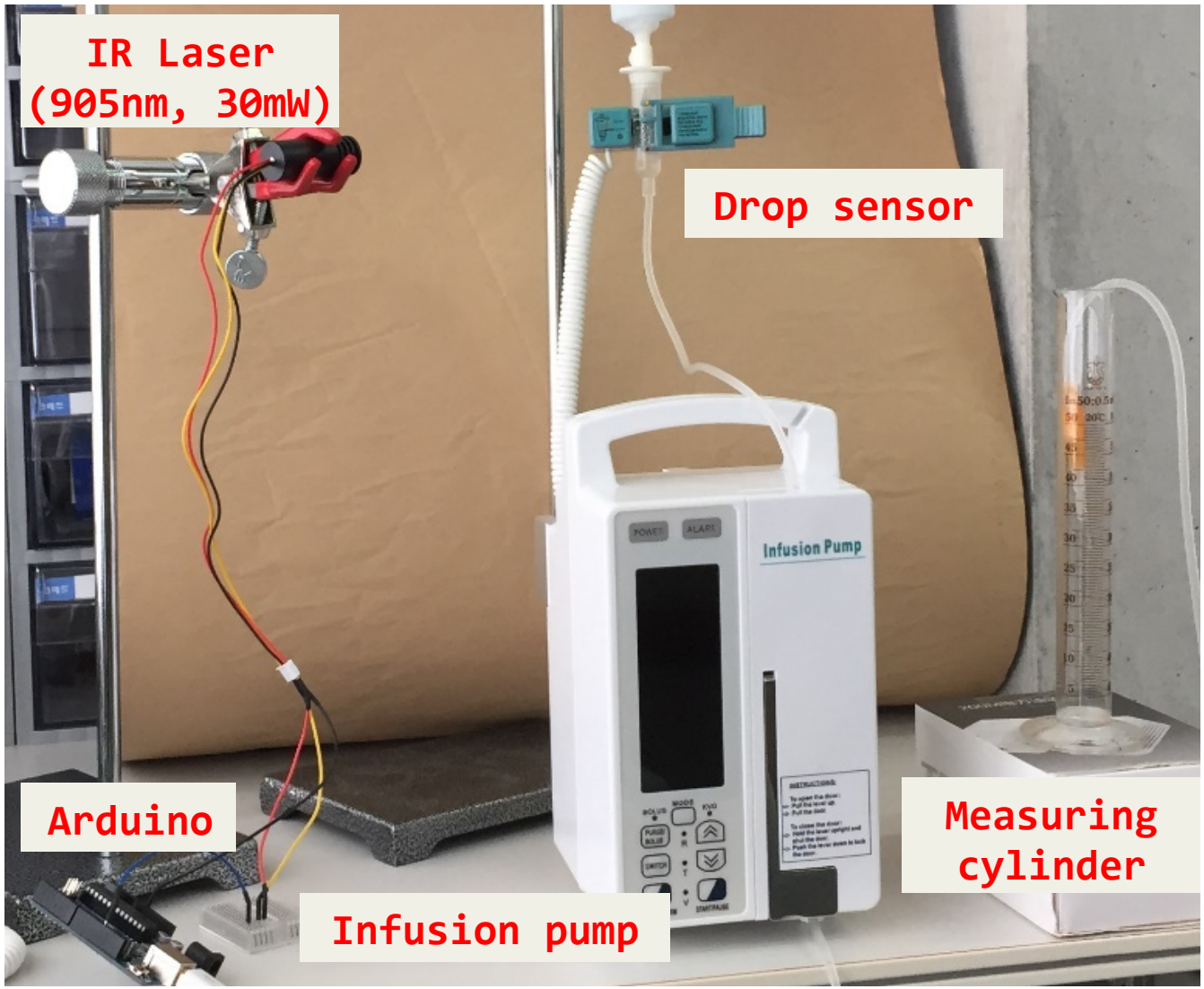


Over and Under Infusion

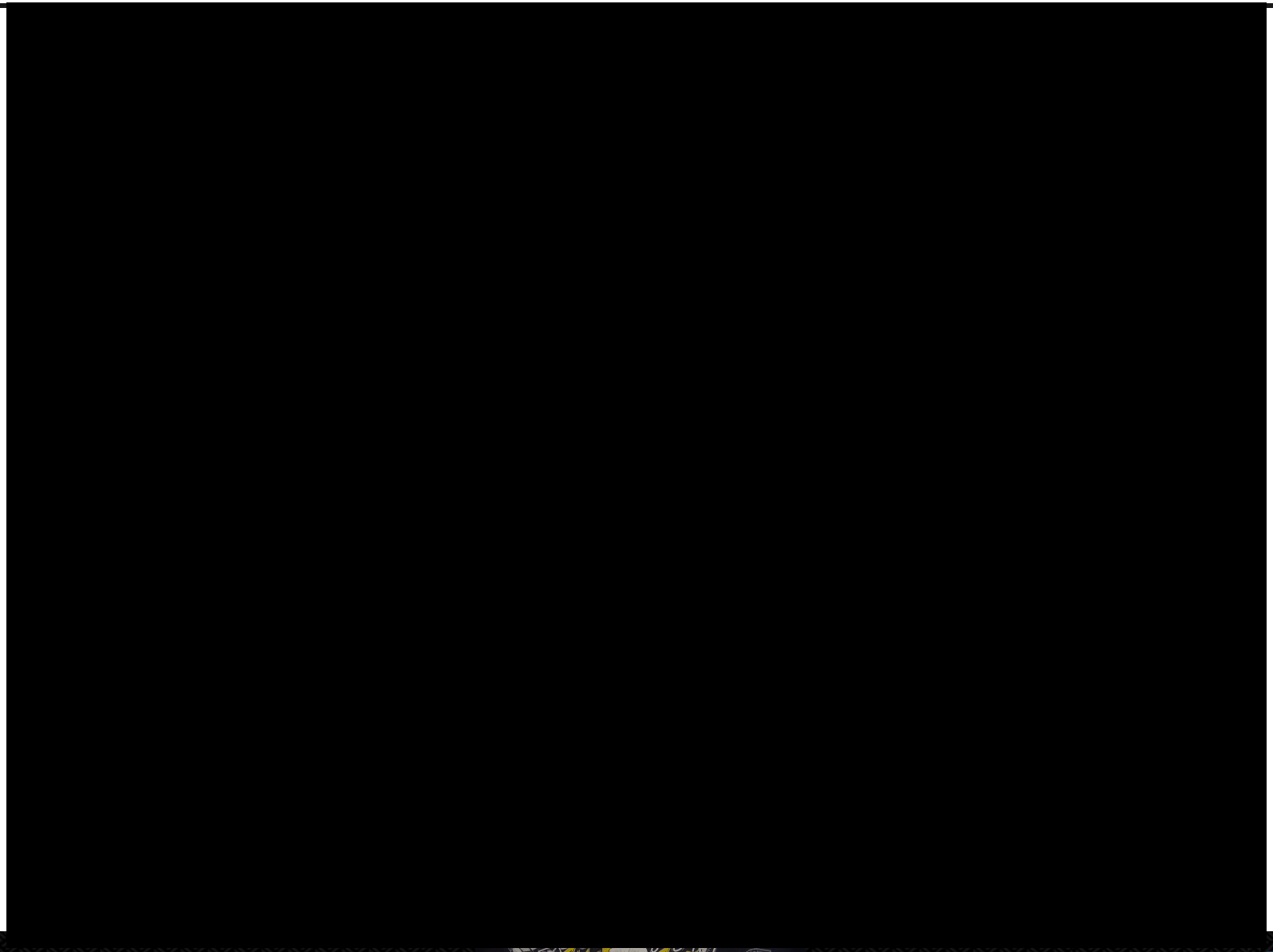


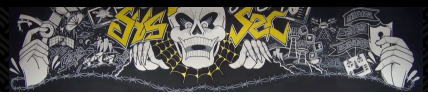


Experimental Setting

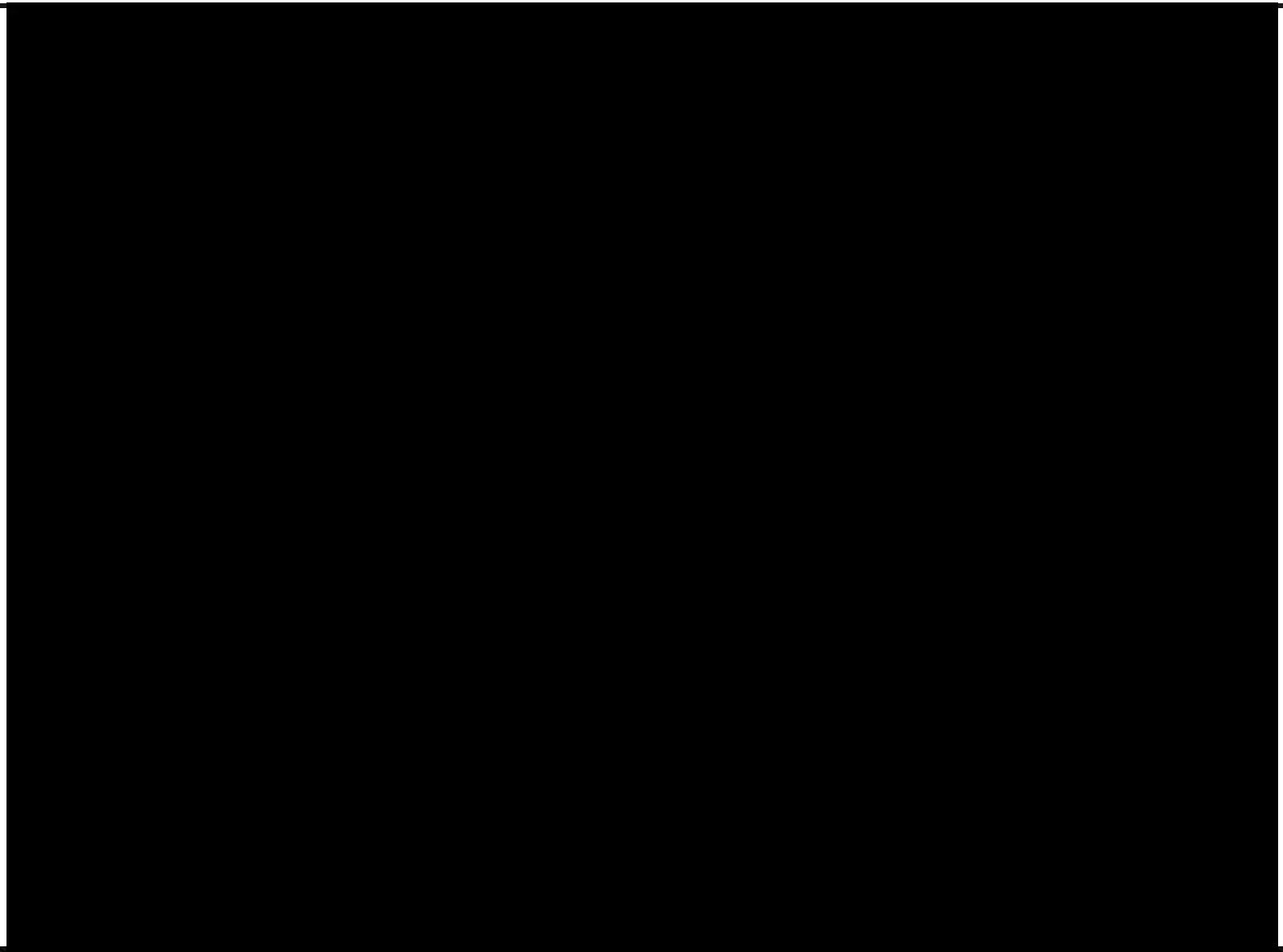


Demo (Over-infusion)



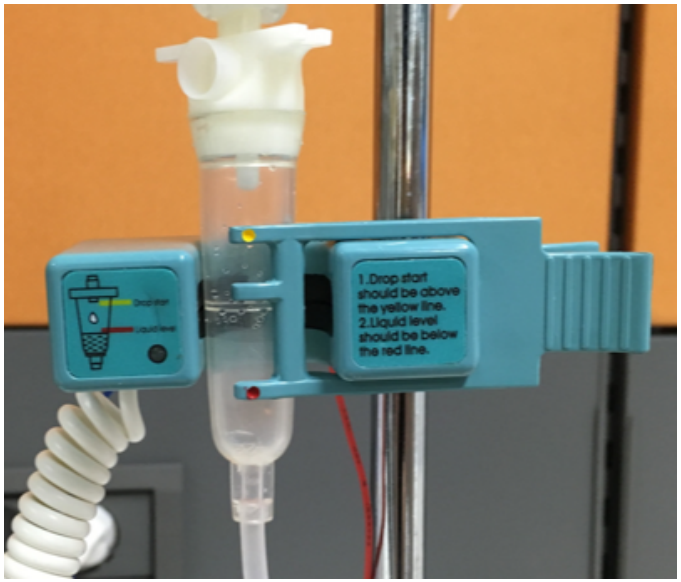


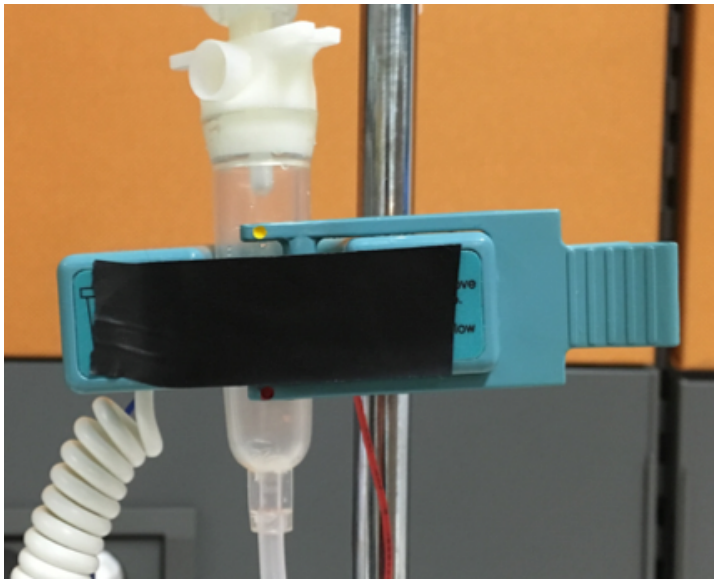
Demo (Under-infusion)



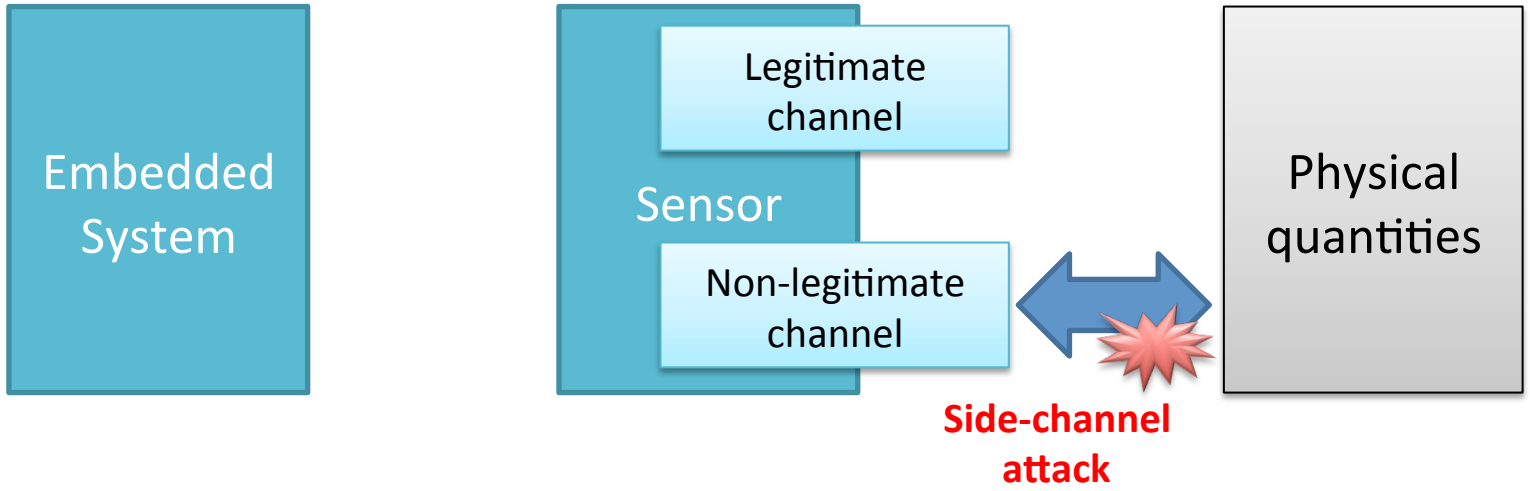


Defense for Sensor Saturation



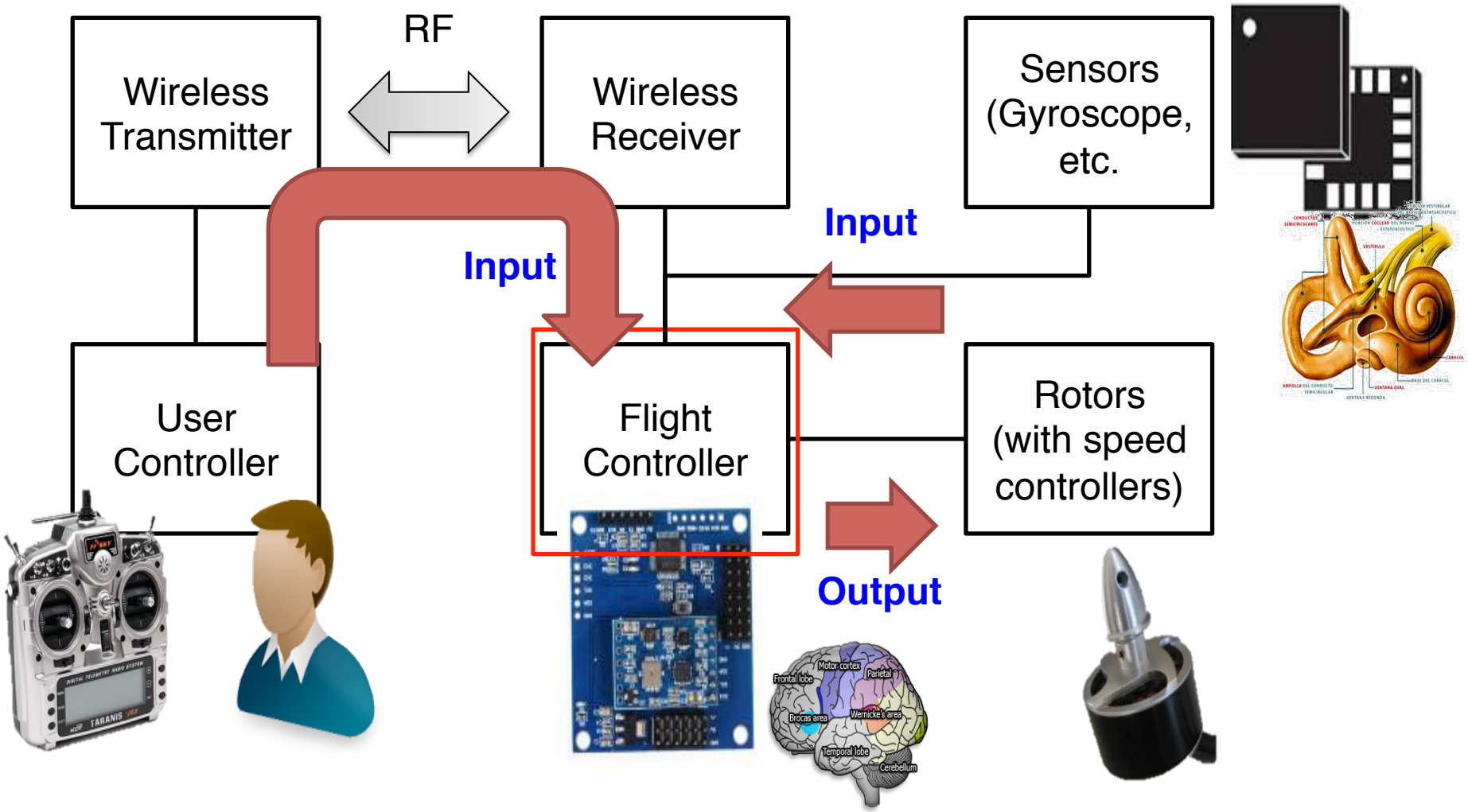


Attack Vectors of Sensors



Insensitive to other physical quantities

Drone Controlling

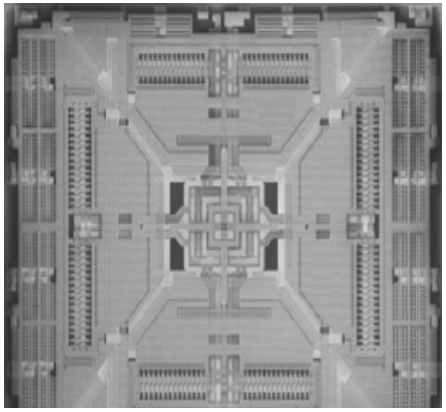


Son et. al. “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors”, Usenix Sec’15

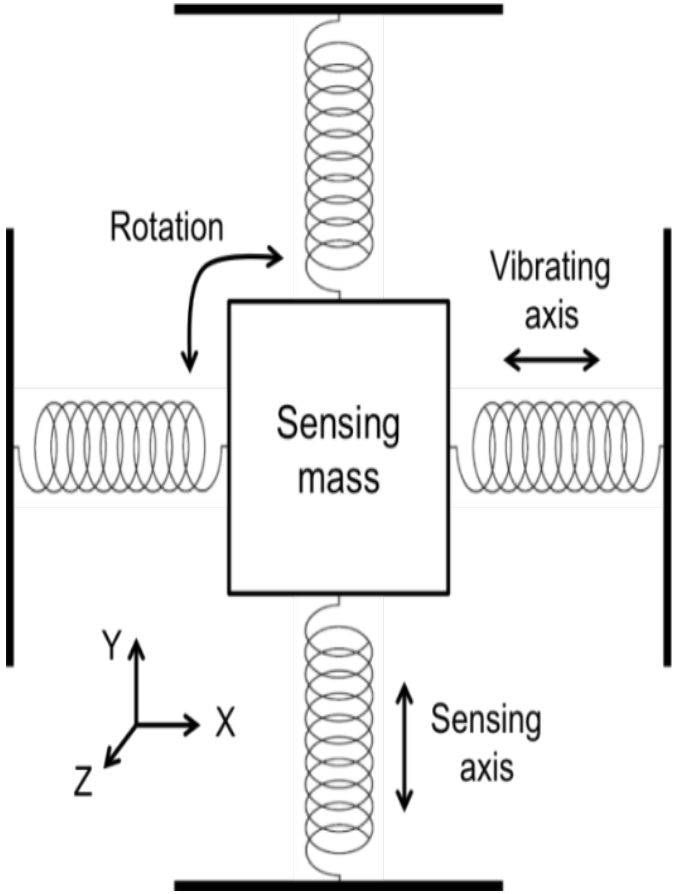
Gyroscope on Drone

- Inertial Measurement Unit (IMU)
  - A device to measure velocity, orientation, or rotation
  - Using a combination of **MEMS gyroscopes** and accelerometers

- MEMS gyroscope

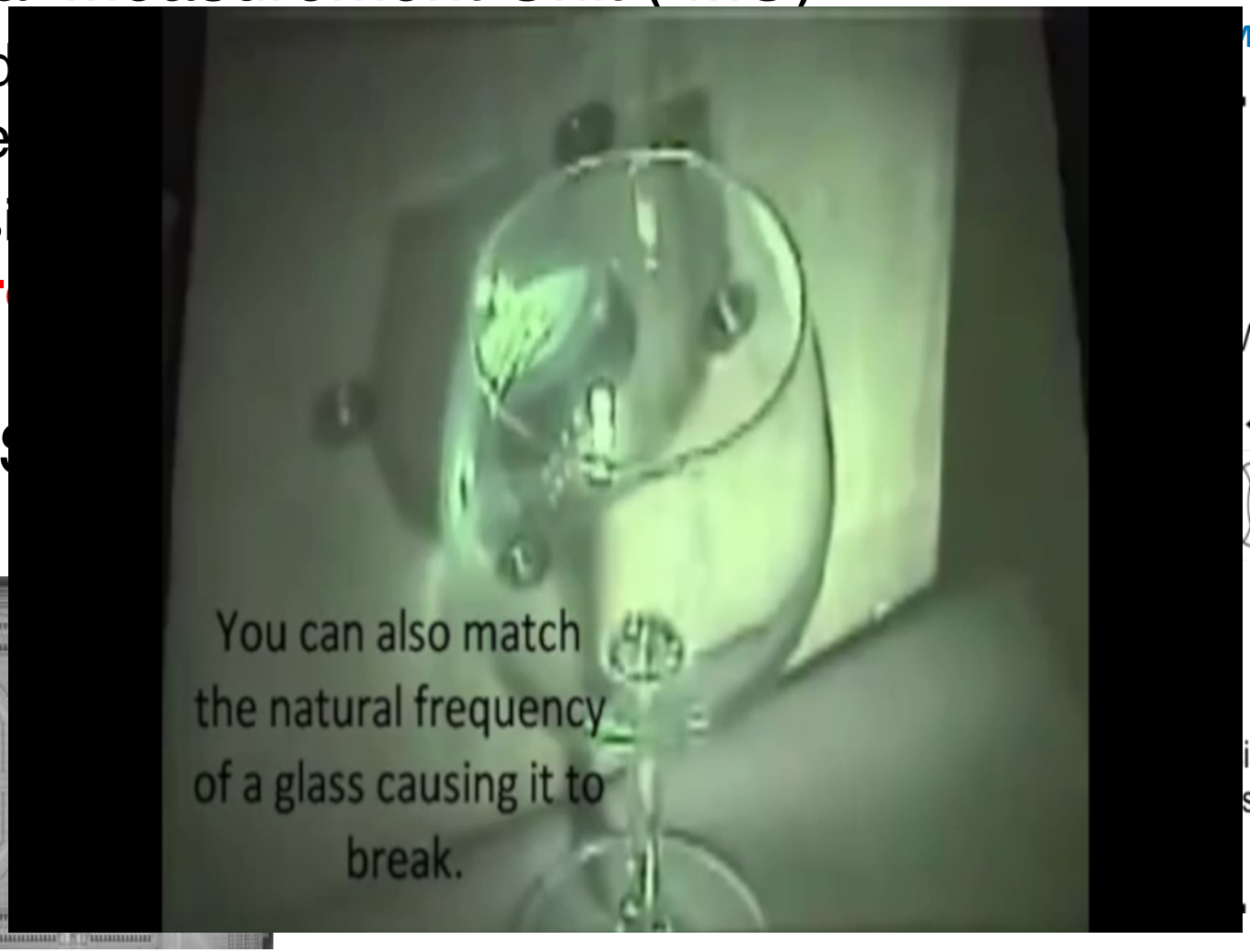


<Conceptual structure of MEMS gyro.>

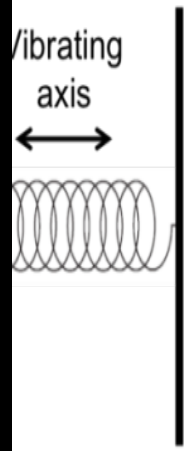


Gyroscope on Drone

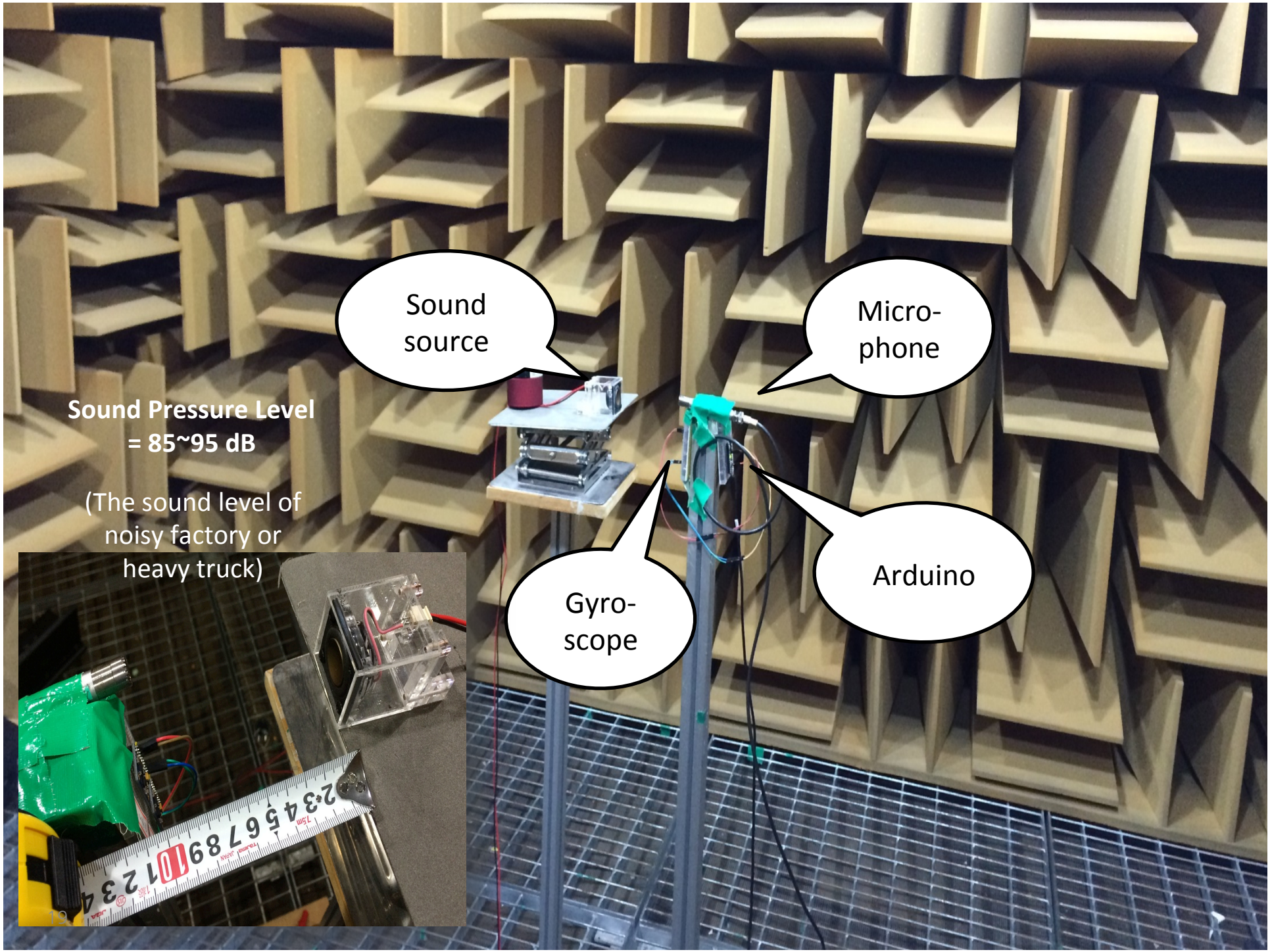
- Inertial Measurement Unit (IMU)
  - A c
    orie
  - Usi
    gyr
- MEM



MS gyro.>



ing
s


Sound source
Micro-phone
Arduino
Gyro-scope
Sound Pressure Level = 85~95 dB
(The sound level of noisy factory or heavy truck)

Experimental Results

- Found the resonant frequencies of **7 MEMS gyroscopes**
- Not found for 8 MEMS gyroscopes

Sensor	Vender	Supporting Axis	Resonant freq. in the datasheet (axis)	Resonant freq. in our experiment (axis)
L3G4200D	STMicro.	X, Y, Z	No detailed information	**7,900 ~ 8,300 Hz (X, Y, Z)**
L3GD20	STMicro.	X, Y, Z		19,700 ~ 20,400Hz (X, Y, Z)
LSM330	STMicro.	X, Y, Z		19,900 ~ 20,000 Hz (X, Y, Z)
MPU6000	InvenSense	X, Y, Z	30 ~ 36 kHz (X) 27 ~ 33 kHz (Y) 24 ~ 30 kHz (Z)	**26,200 ~ 27,400 Hz (Z)**
MPU6050	InvenSense	X, Y, Z		25,800 ~ 27,700 Hz (Z)
MPU9150	InvenSense	X, Y, Z		27,400 ~ 28,600 Hz (Z)
MPU6500	InvenSense	X, Y, Z	25 ~ 29 kHz (X, Y, Z)	26,500 ~ 27,900 Hz (X, Y, Z)



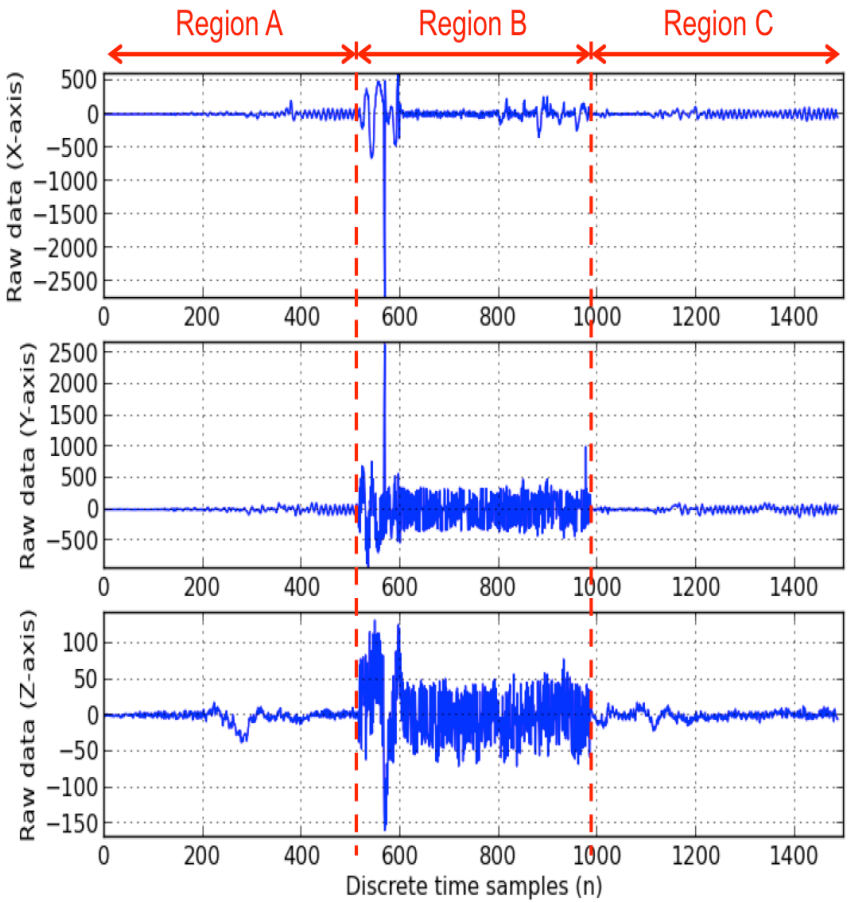
Shutting Down Drones

- Demo Scenario
  - No attack on 10 seconds
  - Playing sound for the next 10 seconds.
  - Turning sound off for the last 10 seconds.

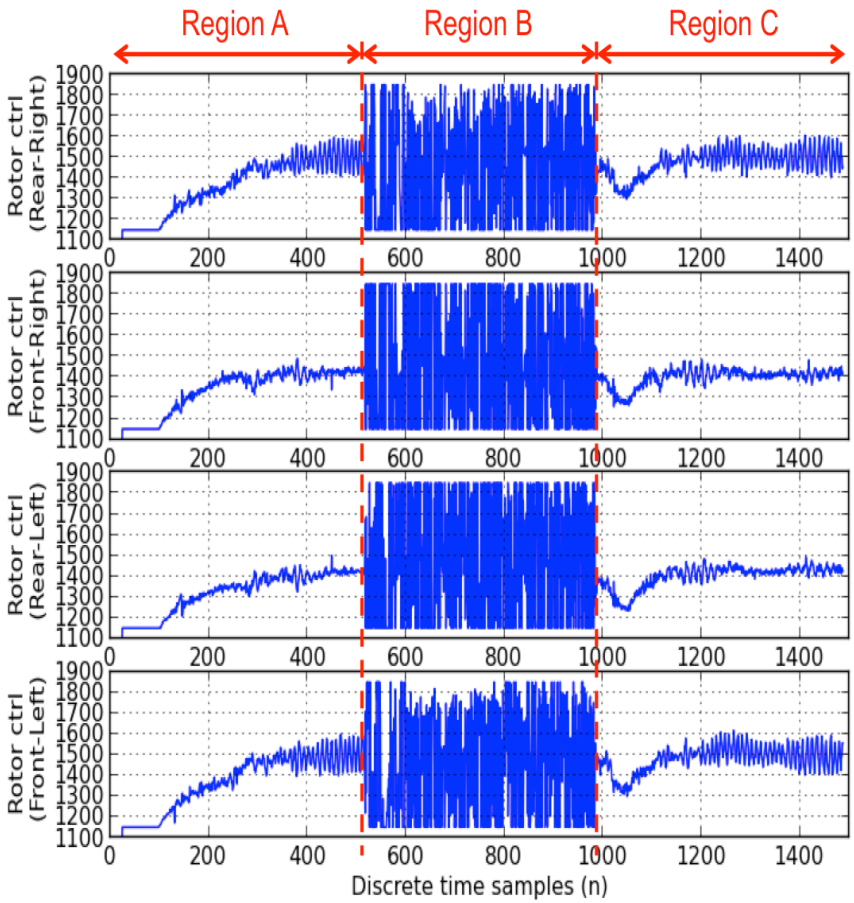




Attack Demo

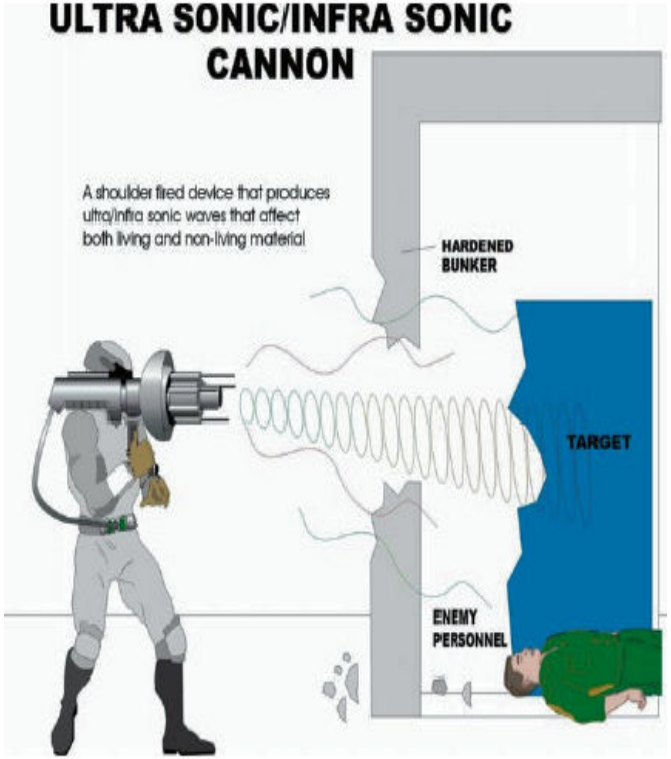


Raw data samples of the gyroscope



Rotor control data samples

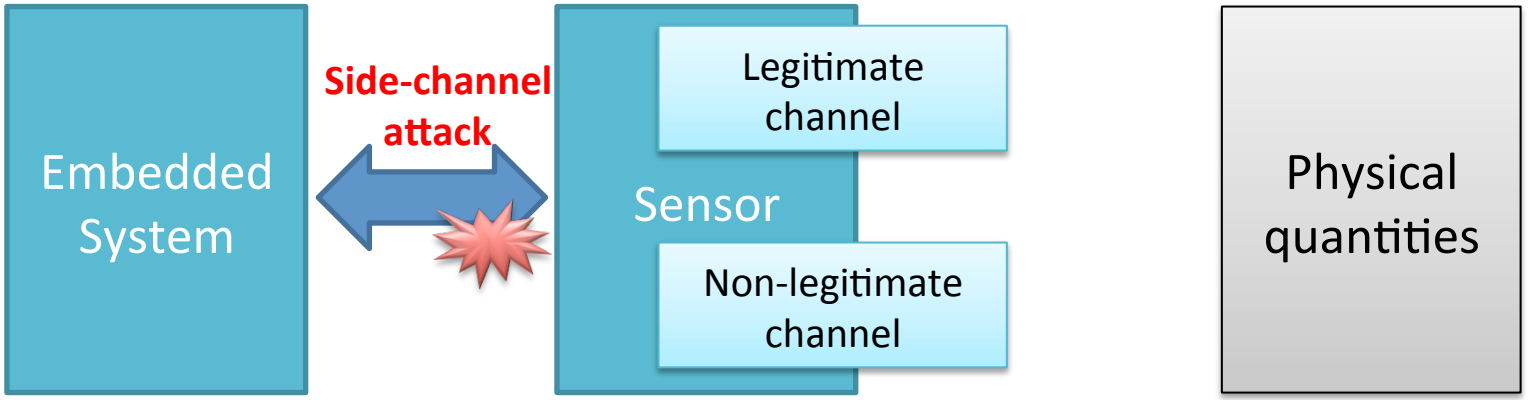
Remote Drone Attack





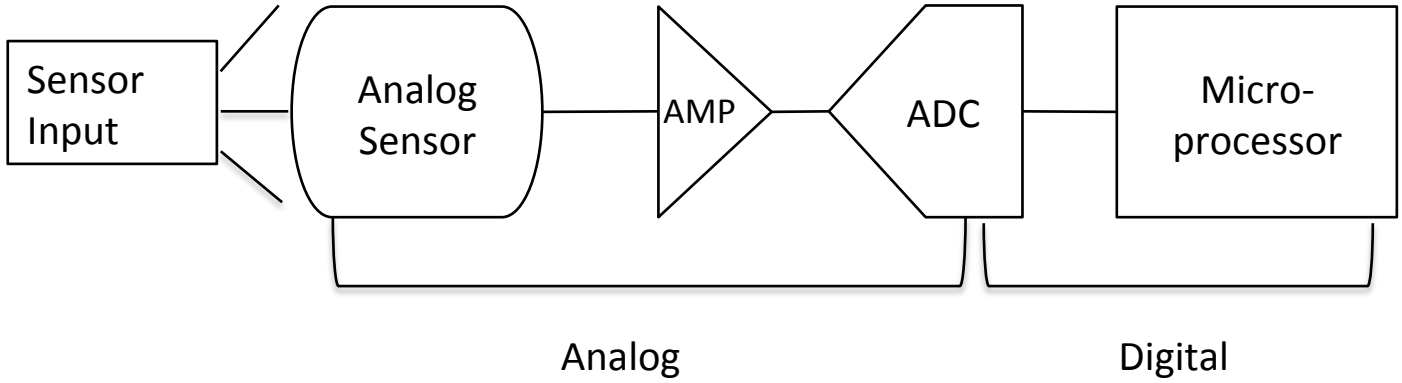


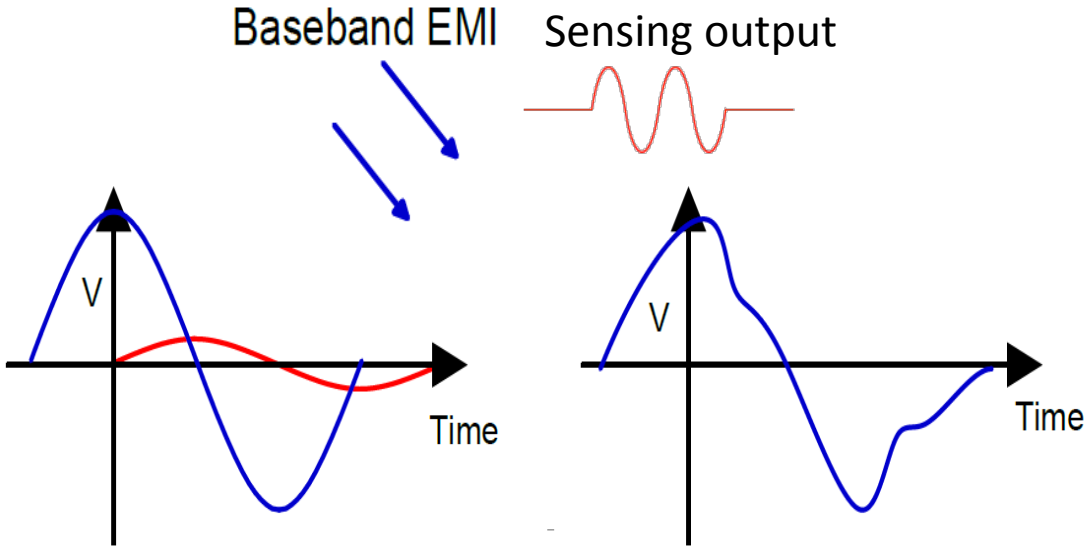
Attack Vectors of Sensors



Need to send sensor data to the system

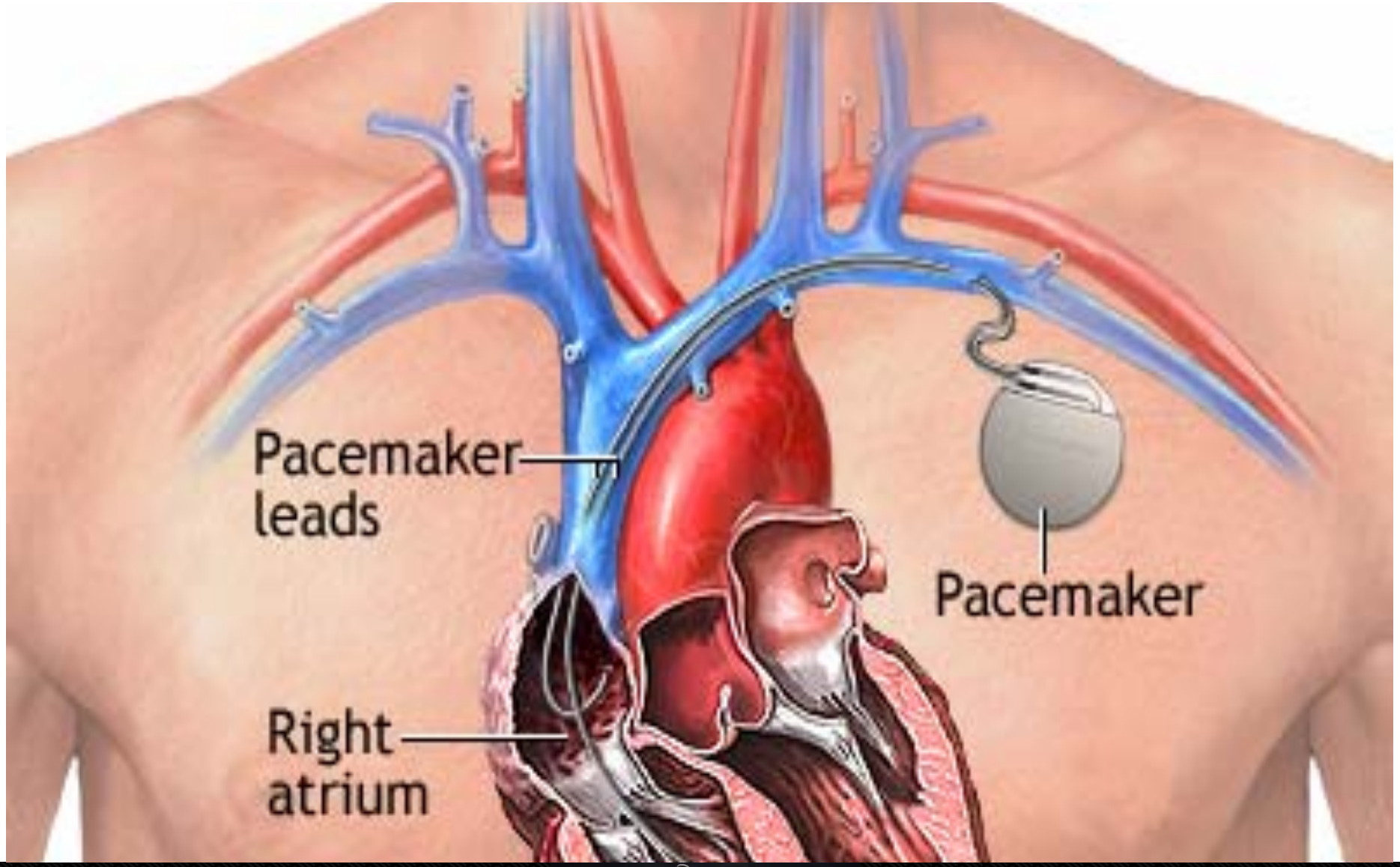
Signal Injection using EMI





Kune, et. al, Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors, IEEE S&P'13

Cardiac Implantable Devices



Application to medical devices

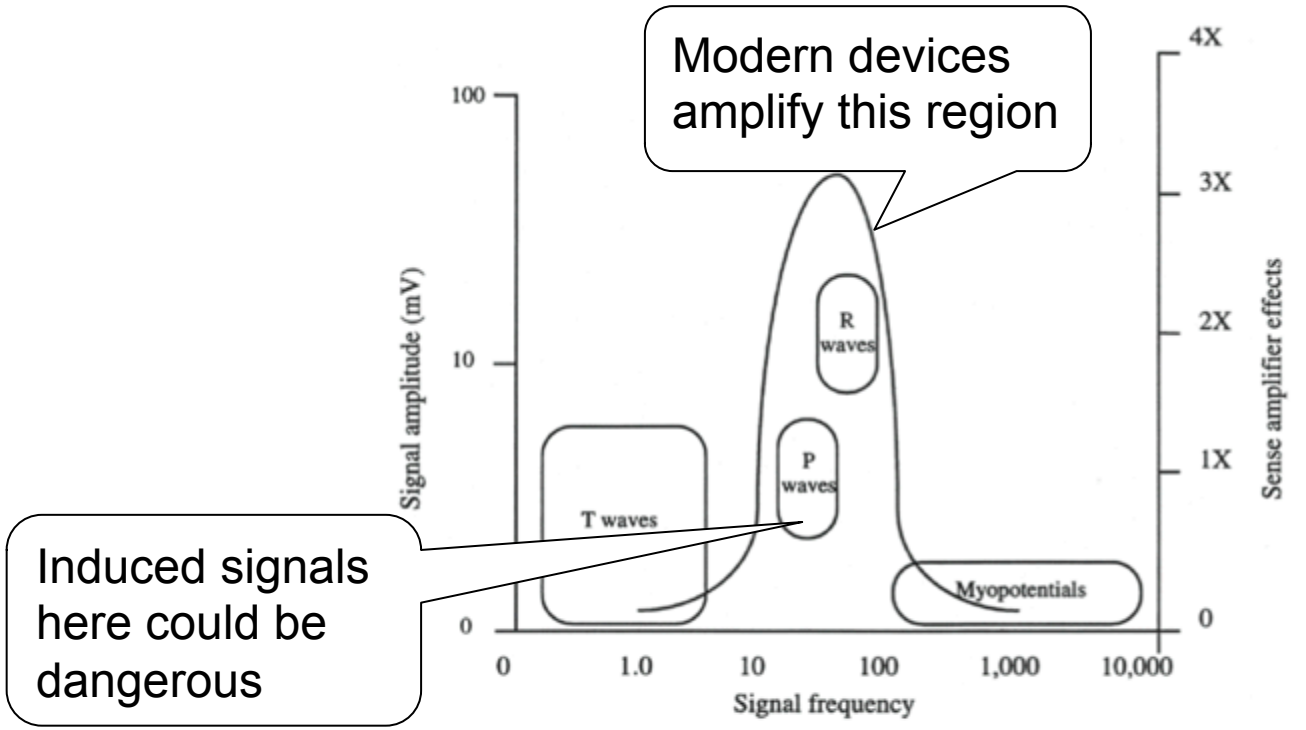


Fig 17.1 Signal amplitude and frequency from various sources. Modern sense amplifiers employ bell-shaped response curves that amplify signals within the 10–100 Hz range while attenuating signals below and above these frequencies. In this way signals from ventricular depolarization (R waves) and atrial depolarization (P waves) can be amplified and the effects from spurious signals, such as T waves and myopotentials, can be minimized.

Standard Lead Design

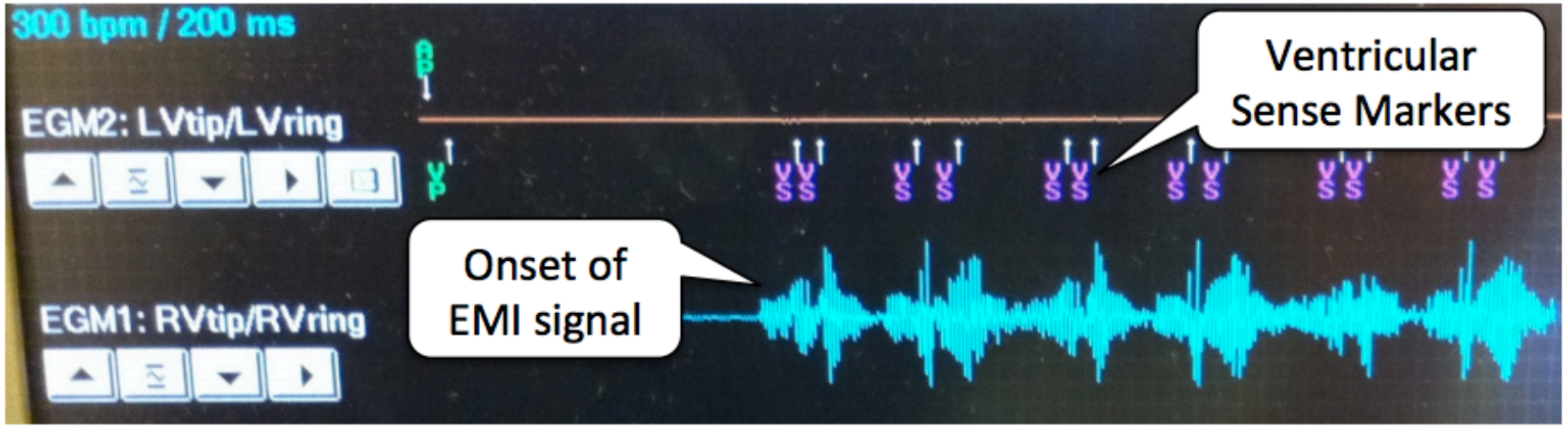


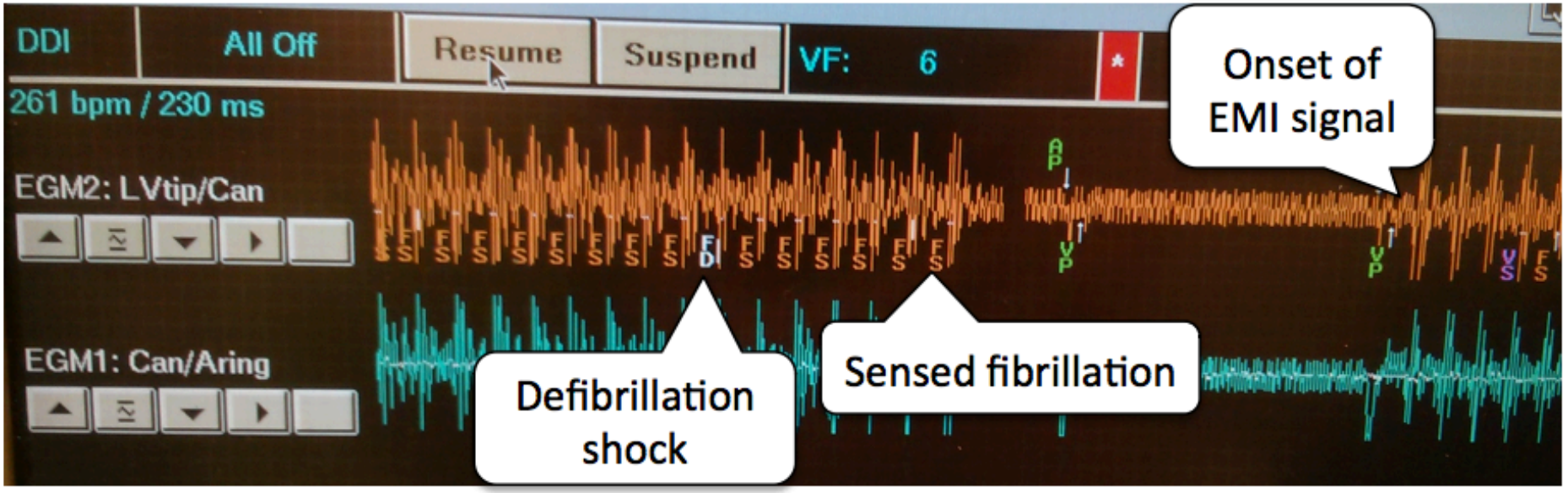
Results

Device	Open air	Saline	SynDaver
Medtronic Adapta	1.40m	0.03m	Untested
Medtronic Insync Sentry	1.57m	0.05m	0.08m
Boston Scientific ICD	1.34m	Untested	Untested
St. Jude ICD	0.68m	Untested	Untested

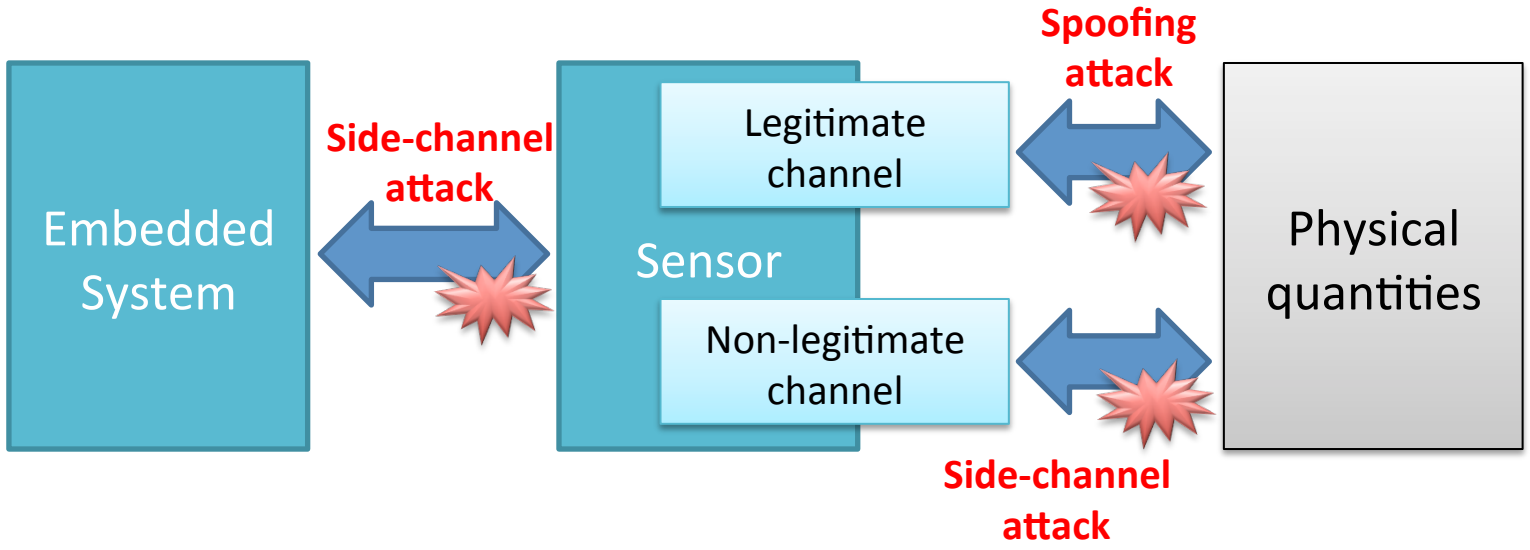


Example


300 bpm / 200 ms
EGM2: LVtip/LVring
EGM1: RVtip/RVring
Ventricular Sense Markers
Onset of EMI signal


DDI
All Off
Resume
Suspend
VF: 6
261 bpm / 230 ms
EGM2: LVtip/Can
EGM1: Can/Aring
Onset of EMI signal
Defibrillation shock
Sensed fibrillation

Attack Vectors of Sensors



Conclusion

- Sensing is one of the most important components of IoT
  - Driverless cars, Drones, Medical devices, SCADA systems, …
- However, so far sensor security has been out of concern
- The mechanism behind sensors are diverse.
  - Electrical, physical, mechanical, chemical, …
- Therefore, the defense against each of the attack depends on its mechanism.
- Now it is time to look at security of sensors.



Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"
- Presented Work
  - Park, Son, Shin, Kim and Kim, This ain't your dose: Sensor Spoofing Attack on Medical Infusion Pump, Usenix WOOT'16
  - Son, Shin, Kim, Park, Noh, Choi, Choi, and Kim "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors", Usenix Sec'15
  - Foo Kune, Backes, Clark, Kramer, Reynolds, Fu, Kim, Xu, "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors", IEEE S&P'13



Adding Sound

