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)
- Sonar (active)
- Magnetometer (passive)
- Gyroscope and accelerometer (passive)
Sensing & Actuation

- Actuation and decision-making based on sensor data

Diagram:
- Real World
- Sensor
  - Gyroscope
  - Radar (RF sensor)
- IoT Devices
  - Glucose sensor
  - Insulin injection
- Actuator
  - Defibrillator
  - Electric shock
  - Flight control
  - Avoid crash
- IoT (Internet of Things) Devices

Diagram shows the integration of sensors and actuators in real-world applications, including medical devices and automotive safety systems.
Diagram not to scale.
Sources: Florida Highway Patrol Troop; U.S. National Highway Traffic Safety Administration
C. Chan, 30/06/2016
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

```c
int led = A1;
int bpm = 100;
int timer = 30000/bpm;

void setup() {
    pinMode(led, OUTPUT);
}

void loop() {
    analogWrite(led, 255);
    delay(timer);
    analogWrite(led, 0);
    delay(timer);
}
```

Exercise situation: attacker set 100 bpm
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

- Sensor output
  - (No drop sensed)
- MCU output

- Real drops (without spoofing)
- Saturation (by spoofing)

- Sensor output
- MCU output

- Fake drops (by spoofing)
Experimental Setting

IR Laser (905nm, 30mW)

Drop sensor

Arduino

Infusion pump

Measuring cylinder
Demo (Over-infusion)
Demo (Under-infusion)
Defense for Sensor Saturation
Attack Vectors of Sensors

- Embedded System
- Sensor
  - Legitimate channel
  - Non-legitimate channel
- Physical quantities

Side-channel attack

Insensitive to other physical quantities
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
Gyroscope on Drone

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

- **MEMS**

---

You can also match the natural frequency of a glass causing it to break.
Sound source

Microphone

Gyro-scope

Arduino

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

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

ULTRA SONIC/INFRA SONIC CANNON

A shoulder fired device that produces ultra/infra sonic waves that affect both living and non-living materials.
Need to send sensor data to the system
Signal Injection using EMI

Sensor Input → Analog Sensor → AMP → ADC → Micro-processor

Baseband EMI → Sensing output

Kune, et. al, Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors, IEEE S&P'13
Cardiac Implantable Devices
Application to medical devices

Modern devices amplify this region

Induced signals here could be dangerous

Fig 17.1. Signal amplitude and frequency from various sources. Modern sense amplifiers employ bell-shaped response curves that amplify signals within the 10–100Hz 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

Anode

Cathode
## Results

<table>
<thead>
<tr>
<th>Device</th>
<th>Open air</th>
<th>Saline</th>
<th>SynDaver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medtronic Adapta</td>
<td>1.40m</td>
<td>0.03m</td>
<td>Untested</td>
</tr>
<tr>
<td>Medtronic Insync Sentry</td>
<td>1.57m</td>
<td>0.05m</td>
<td>0.08m</td>
</tr>
<tr>
<td>Boston Scientific ICD</td>
<td>1.34m</td>
<td>Untested</td>
<td>Untested</td>
</tr>
<tr>
<td>St. Jude ICD</td>
<td>0.68m</td>
<td>Untested</td>
<td>Untested</td>
</tr>
</tbody>
</table>
Example

- Ventricular Sense Markers
- Onset of EMI signal
- Defibrillation shock
- Sensed fibrillation

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
Attack Vectors of Sensors

- **Embedded System**
- **Sensor**
  - Legitimate channel
  - Non-­‐legitimate channel
- **Physical quantities**

Attack vectors include:
- Side-­‐channel attack
- Spoofing attack
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
Adding Sound