We thank our shepherd Prof. Brendan Dolan-Gavitt and the anonymous reviewers for their constructive feedback. This work was supported in part by the ZJU-OPPO-OnePlus Joint Innovation Center, NSF CNS-1330142, a gift from Analog Devices Inc., and by an award from Mcity at University of Michigan. The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the ZJU-OPPO-OnePlus Joint Innovation Center, NSF, Analog Devices, or Mcity.
Sensors are everywhere!

Manufacturing

IMU and Magnetometer
Forward Vision Sensors
Camera

Drones

Ultrasonic and Bottom Vision Sensors

Automotive

Infrared

IoT

S&P 2020
SoK: A Minimalist Approach to Formalizing Analog Sensor Security
Transduction Attacks:

Attacks that use physical signals to induce untrustworthy sensor output

The New York Times

With a Laser, Researchers Say They Can Hack Alexa, Google Home or Siri


The New York Times

It’s Possible to Hack a Phone With Sound Waves, Researchers Show


New attack on autonomous vehicle sensors creates fake obstacles


Sounds can knock drones out of the sky

Transduction Attacks: Challenges

Sensors are ubiquitous and heterogeneous

**Varying** attack signals, sensors, goals

Vocabulary and terminology differences

*We found that there were conceptual similarities, but we lacked a simple way to express those similarities.*
Contributions:

1. Simple Sensor Security Model
2. Tranduction attack systemization
3. Defense systemization
4. Prediction methodology for attacks and defenses.
What are commonly inside a sensor?

Stimulus → Input → Sensor → Measurement

Transducer → Amplifier → Filter → ADC (Analog to digital converter)

Physical signal → Analog signal → Digital signal

Speech → Audio file

0101...
How do transduction attacks work?

**Stimulus**

- Malicious Physical Signals:
  - 1. RF signals
  - 2. Acoustic signals
  - 3. Light
  - 4. Magnet
  - 5. Heat

**Sensor**

- Input
- Transducer
- Amplifier
- Filter
- ADC (Analog to digital converter)

**Measurement**

- Output: 0111...
Simple Sensor Security Model
General Ideas

**Common Properties**
1. Similar analog signal processing
2. Same signal modalities
3. Sensitive to physical signals
4. Chain of blind trust

**Sensor Model**
Model each sensor component with a transfer function

**Adversary in the Model**
Model attacks by adding malicious signals into the model

- **Input** → \( f_i \) → **Output**
- **Legitimate input** → \( f_i \) → **Output**
- **Malicious input** → \( f_i \) → **Output**
Simple Sensor Security Model
Transfer Function Representation

\[
\begin{align*}
\text{Stimulus} & \rightarrow f_1 \rightarrow f_i \rightarrow f_m \rightarrow \text{Measurement} \\
\begin{array}{c}
\text{Input} \quad \text{Transducer} \\
\text{Sensor} \quad \text{Amplifier} \\
\text{Filter} \quad \text{ADC} \\
\text{Output} \quad 0101...
\end{array}
\end{align*}
\]

\[
\text{Stimulus} \quad x_1 \quad x_2 \quad \ldots \quad x_i \quad \ldots \quad x_m \\
\text{Noise} \quad n_1 \quad n_i \quad \ldots \quad n_m \\
\text{Measurement} \quad y = \mathcal{F}(x_1, n) \quad n = [n_1, \ldots, n_m]
\]
Simple Sensor Security Model
Transfer Function Representation: Microphone Example

\[ y = \mathcal{F}(x_1, n) \]
\[ n = [n_1, \ldots, n_4] \]
Simple Sensor Security Model
Adversaries in the Model

Stimulus
Noise

\[ \begin{align*}
    x_1 & \to f_1 \\
    x_2 & \to f_2 \\
    \vdots & \to \vdots \\
    x_i & \to f_i \\
    \vdots & \to \vdots \\
    x_m & \to f_m \\
\end{align*} \]

Measurement
\[ y = F(x_1, n) \]
\[ n = [n_1, \ldots, n_m] \]

\[ \begin{align*}
    x_1 & \to f_1 \\
    x_2 & \to f_2 \\
    \vdots & \to \vdots \\
    x_i & \to f_i \\
    \vdots & \to \vdots \\
    x_m & \to f_m \\
\end{align*} \]

Desired Measurement
\[ y' = F(x_1, n + a) \]
\[ a = [a_1, \ldots, a_m] \]

Desired value of y
Sensor knowledge

Malicious Inputs
\[ \begin{align*}
    a_1 & \to f_1 \\
    \cdots & \to \cdots \\
    a_i & \to f_i \\
    \cdots & \to \cdots \\
    a_m & \to f_m \\
\end{align*} \]
Simple Sensor Security Model
Example: DolphinAttack (Zhang et al., CCS 2017)
Attack Systemization
Common Attack Steps

Step 1: Signal Injection

Step 2: Measurement Shaping
Attack Systemization
Signal Injection Step (3 factors)

**Injection Point**
- **Pre-transducer**
  - Sensor: MEMS Inertial Sensor
    - Expected Operating Band: \( \leq 750 \text{ Hz} \)
    - Attack Frequency: \( > 1\text{kHz} \)
  - Sensor: Microphone
    - Expected Operating Band: \( \leq 20 \text{ kHz} \)
    - Attack Frequency: \( > 20 \text{kHz} \)

- **Post-transducer**
  - Signal Type: RF signal

**Signal Type**
- **Pre-transducer**: RF signal, light, sound, magnetic, electric...
- **Post-transducer**: RF signal

**Signal Frequency**
- In-band vs. out-of-band
  - MEMS Inertial Sensor
    - Expected Operating Band: \( \leq 750 \text{ Hz} \)
    - Attack Frequency: \( > 1\text{kHz} \)
  - Microphone
    - Expected Operating Band: \( \leq 20 \text{ kHz} \)
    - Attack Frequency: \( > 20 \text{kHz} \)
Attack Systemization
Measurement Shaping Step (5 types)

- **Saturation**
- **Aliasing**
- **Filtering**

**Intermodulation Distortion**

**Envelope Detection**
Attack Systemization

Example: ① DolphinAttack & ② Ghost Talk

1. **Injection:** Ultrasound
   - Pre-transducer
   - Out-of-band

2. **Injection:** RF signal
   - Post-transducer
   - Out-of-band

**IMD:** Demodulate attack signal

**Filtering:** Remove attack signal

**Input**

Microphone → Amplifier → LPF → ADC → **Output**

Malicious Audio
## Attack Systemization

### Summary

<table>
<thead>
<tr>
<th>Application</th>
<th>Sensor Type</th>
<th>Exploited Component</th>
<th>Signal Injection Steps</th>
<th>Measurement Shaping Steps</th>
<th>Outcome</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automobile</td>
<td>Lidar</td>
<td>A</td>
<td>Pre ⚫ In</td>
<td>Sat. IMD, Fil., Env., Ali.</td>
<td>⬤</td>
<td>[45]</td>
</tr>
<tr>
<td></td>
<td>Camera</td>
<td>F</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
<td>[46], [70]</td>
</tr>
<tr>
<td></td>
<td>Radar</td>
<td>A</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
<td>[70]</td>
</tr>
<tr>
<td></td>
<td>Ultrasonic Sensor</td>
<td>A</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
<td>[68], [70]</td>
</tr>
<tr>
<td></td>
<td>Magnetic Encoder</td>
<td>A</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
<td>[96], [97]</td>
</tr>
</tbody>
</table>

### Table II: Systematization of Transduction Attacks with the Simple Sensor Security Model

<table>
<thead>
<tr>
<th>Sensor Categories</th>
<th>Exploited Component</th>
<th>Signal Inject Steps</th>
<th>Measurement Shaping Steps</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microphone</td>
<td>F</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Touchscreen</td>
<td>A</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>MEMS Shock Sensor</td>
<td>Pre ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Energy</td>
<td>Infrared Sensor</td>
<td>Post ⚫ Out</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Medical Devices</td>
<td>Pacemaker Lead</td>
<td>Post ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td></td>
<td>Debrillator Lead</td>
<td>Post ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td></td>
<td>Drop Counter</td>
<td>Post ⚫ In</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Active sensor</th>
<th>Passive sensor</th>
<th>Pre-transducer</th>
<th>Post-transducer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visable</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>RF</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Audible</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Magnetic</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Electric</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Trans. Wire</th>
<th>Ampl. Filter</th>
<th>ADC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>F</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>A</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>A</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>[45]</td>
</tr>
<tr>
<td>[46]</td>
</tr>
<tr>
<td>[70]</td>
</tr>
<tr>
<td>[68], [70]</td>
</tr>
<tr>
<td>[96], [97]</td>
</tr>
<tr>
<td>[103]</td>
</tr>
<tr>
<td>[86]</td>
</tr>
<tr>
<td>[75], [76]</td>
</tr>
<tr>
<td>[47]</td>
</tr>
<tr>
<td>[87]</td>
</tr>
</tbody>
</table>
Defense Systemization
Detection and Prevention

Ghost Talk

Detection

Prevention
Defense Systematization:
Detection

Injection

TX Randomization

Verifying Actuation

Detecting Out-of-band

Measurement Shaping

Saturation Detection

IMD Feature Detection
Defense Systematization:
Prevention

- Randomization
- Shielding
- Filtering
- Fusion
- Component Quality Improvement
# Defense systematization

## TABLE III: Systematization of Transduction Attack Defenses

<table>
<thead>
<tr>
<th>Goal</th>
<th>Category and Subcategory</th>
<th>Related Component(s)</th>
<th>Injection and Shaping Steps</th>
<th>Xfer Function</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inject</td>
<td>TX randomiz.</td>
<td>TX Trans., Wire, Amp., Fil., ADC, Dig.</td>
<td>Both</td>
<td>Both</td>
<td>[68], [87], [106]</td>
</tr>
<tr>
<td></td>
<td>Verif. Actuation</td>
<td>TX trans., Wire, Amp., Fil., ADC, Dig.</td>
<td>Both</td>
<td>Both</td>
<td>[47], [107]</td>
</tr>
<tr>
<td></td>
<td>Detect OOB Sig.</td>
<td>TX trans., Wire, Amp., Fil., ADC, Dig.</td>
<td>Pre</td>
<td>Out</td>
<td>[44], [86]</td>
</tr>
</tbody>
</table>

1 Denotes the three xfer func. models of Section V-B. 2 Digital Backend 3 Attack Surface Reduction
Prediction: Attacks
Example: Part ① DolphinAttack

Injection: Ultrasound
Pre-transducer
Out-of-band

IMD: Demodulate attack signal

Filtering: Remove attack signal

Input
Microphone
Amplifier
LPF
ADC
ADC
Output

Malicious Audio
Prediction: Attacks
Example: Part ② Walnut

Injection: Sound
Pre-transducer
Out-of-band

Filtering: Improper Filtering

Aliasing: ADC aliases signal

Malicious Acceleration
Prediction: Attacks

Example: Part ③ predicting an attack

- **Injection:** Ultrasound
  - Pre-transducer
  - Out-of-band

**Attacker Methods for AM Demodulation**

- **IMD:** Demodulate attack signal
- **Filtering:** Remove attack signal
- **Filtering:** Improper Filtering
- **Aliasing:** ADC aliases signal

**Predict**

- **Injection:** Ultrasound
  - Pre-transducer
  - Out-of-band
- **Filtering:** Improper Filtering
- **Aliasing:** ADC aliases signal
Prediction: Defenses
Example: ① DolphinAttack & ② Ghost Talk

1. Injection: Ultrasound (Pre-transducer, Out-of-band)
   - IMD: Demodulate attack signal
   - Filtering: Remove attack signal
   - Established Defense: Filtering to remove IMD

2. Injection: RF signal (Post-transducer, Out-of-band)
   - IMD: Demodulate attack signal
   - Filtering: Remove attack signal
   - Predicted Defense: Filtering to remove IMD
Conclusion

1. Simple Sensor Security Model enables easier comparison of transduction attacks
2. Our systemization reveals how several attacks and defenses on different sensors can be conceptually similar
3. Analysis of past attacks via our model hints at future attacks and how to defend against them
SoK: A Minimalist Approach to Formalizing Analog Sensor Security

Join us afterwards for a discussion on sensor security!

Contact the authors at:
yanchen@zju.edu.cn
h.c.shin@kaist.ac.kr
mcbolto@umich.edu

Lab websites:
usslab.org
syssec.kr
spqr.eecs.umich.edu

Author websites:
connorbolton.com
sites.google.com/site/hocheolshin

cyans.cn

We thank our shepherd Prof. Brendan Dolan-Gavitt and the anonymous reviewers for their constructive feedback. This work was supported in part by the ZJU-OPPO-OnePlus Joint Innovation Center, NSF CNS-1330142, a gift from Analog Devices Inc., and by an award from Mcity at University of Michigan. The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the ZJU-OPPO-OnePlus Joint Innovation Center, NSF, Analog Devices, or Mcity.