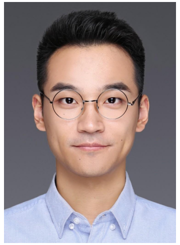
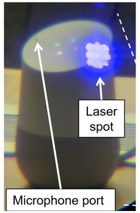
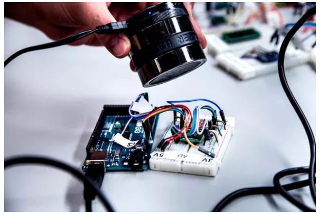
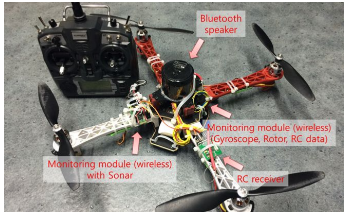
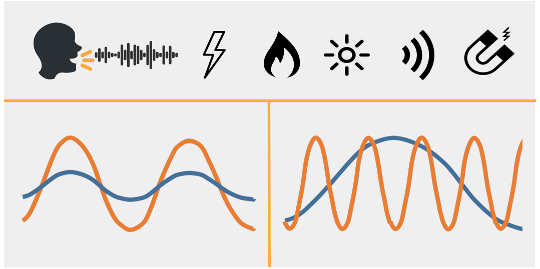
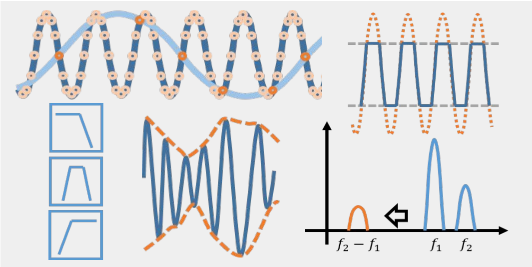
SoK: A Minimalist Approach to Formalizing Analog Sensor Security





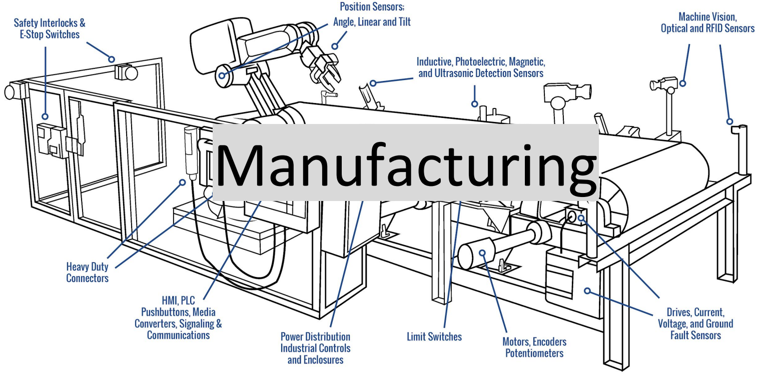



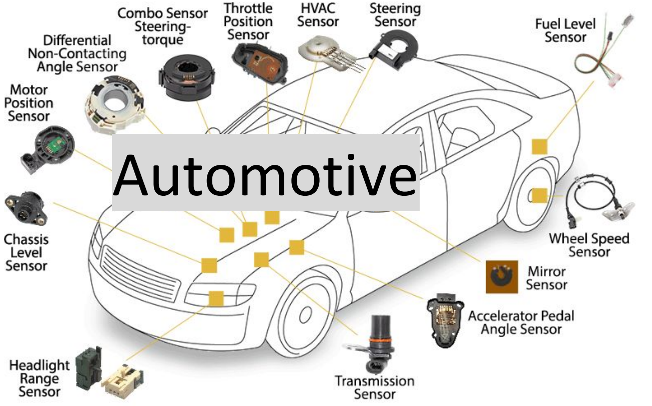



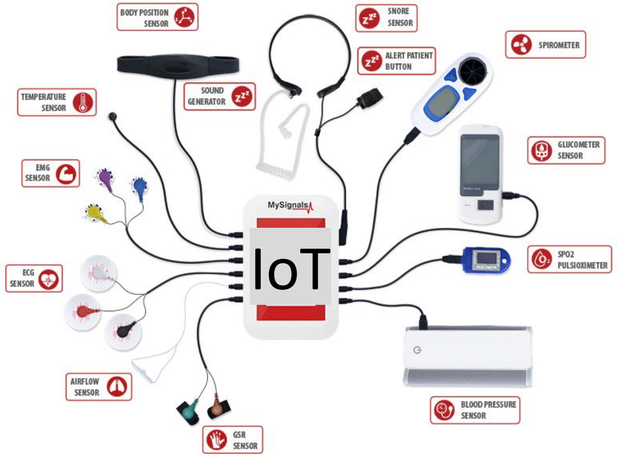
Chen Yan, Hocheol Shin, Connor Bolton,
Wenyuan Xu, Yongdae Kim, Kevin Fu

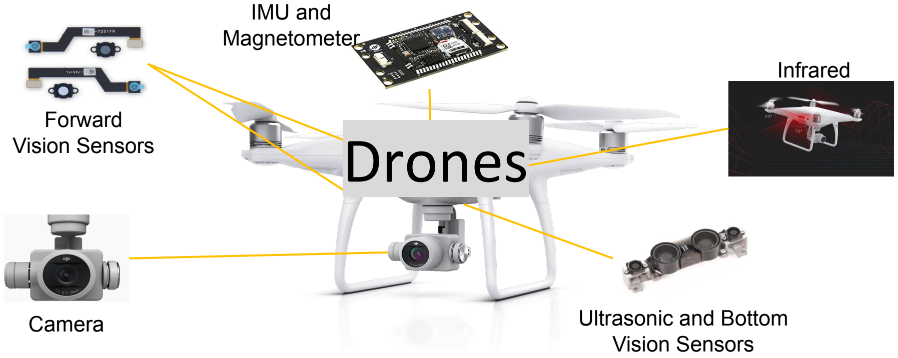
We thank our shepherd Prof. Brendan Dolan-Gavit and the anonymous reviewers for their constructive feedback. This work was supported in part by the ZJU-OPPO-OnePlus Joint Innovation Center, NSF CNS-1330142, a gift from Analog Devices Inc., and by an award from Mcity at University of Michigan. The views 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!



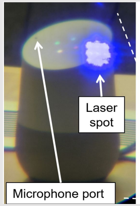






Transduction Attacks:

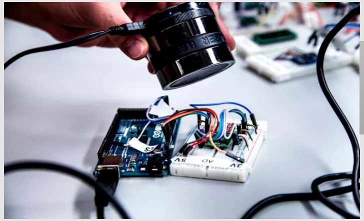
Attacks that use physical signals to induce untrustworthy sensor output



The New York Times

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

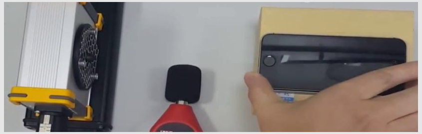
Sugawara, Takeshi, et al. “Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems.”



The New York Times

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

Trippel, Timothy, et al. "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks." *IEEE EuroS&P, 2017*



Zhang, Guoming, et al. "DolphinAttack: Inaudible voice commands." *ACM CCS* 2017.

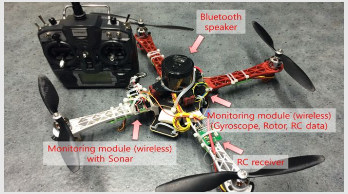
MIT Technology Review

Secret Ultrasonic Commands Can Control Your Smartphone, Say Researchers

Smart devices are vulnerable to inaudible voice attacks.

New attack on autonomous vehicle sensors creates fake obstacles

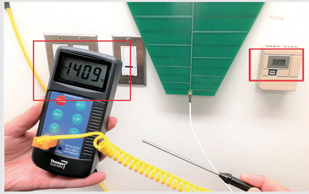
Cao, Yulong, et al. "Adversarial sensor attack on lidar-based perception in autonomous driving." *ACM CCS*, 2019.



Sounds can knock drones out of the sky

PCWorld NEWS

Son, Yunmok, et al. "Rocking drones with intentional sound noise on gyroscopic sensors." *USENIX* 2015.



COMMUNICATIONS OF THE ACM | FEBRUARY 2018

DOI:10.1145/3176402

Inside Risks

Risks of Trusting the Physics of Sensors

Protecting the Internet of Things with embedded security.

Transduction Attacks:
Challenges

Sensors are **ubiquitous and heterogeneous**

Varying attack signals, sensors, goals

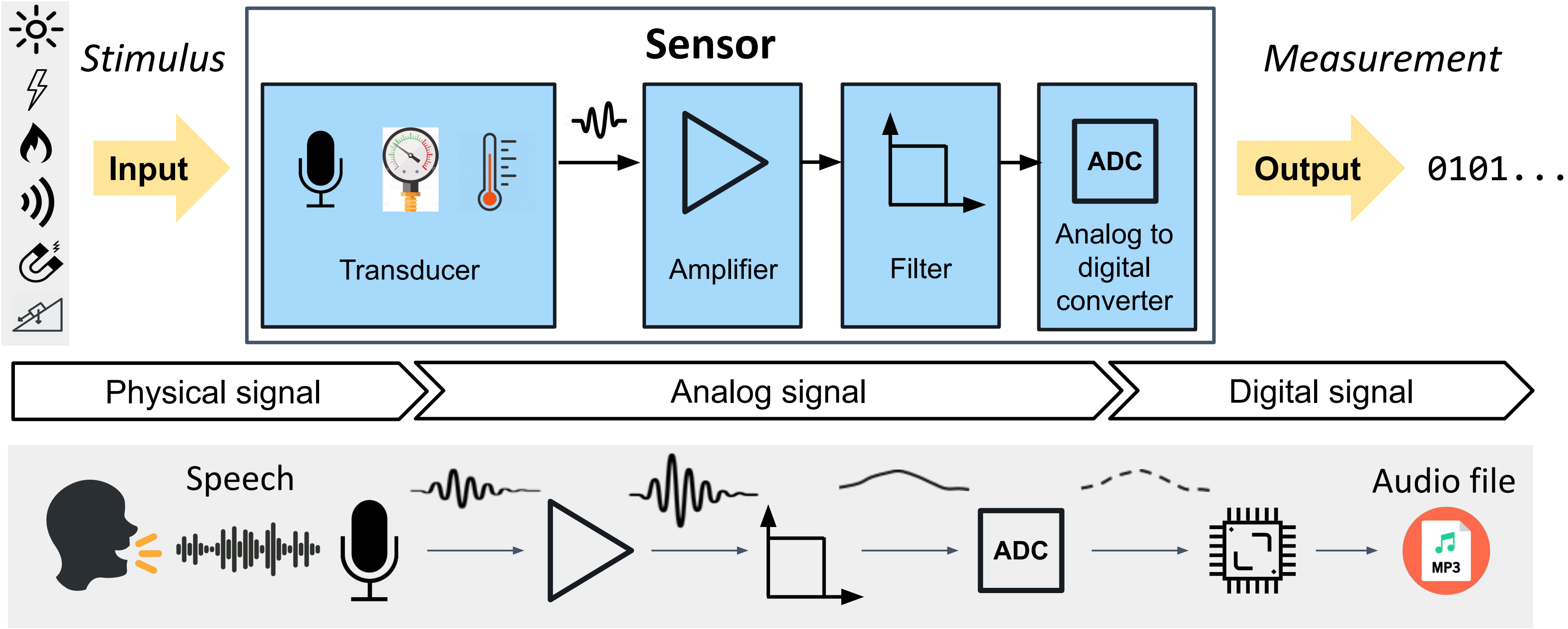
Vocabulary and terminology **differences**

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

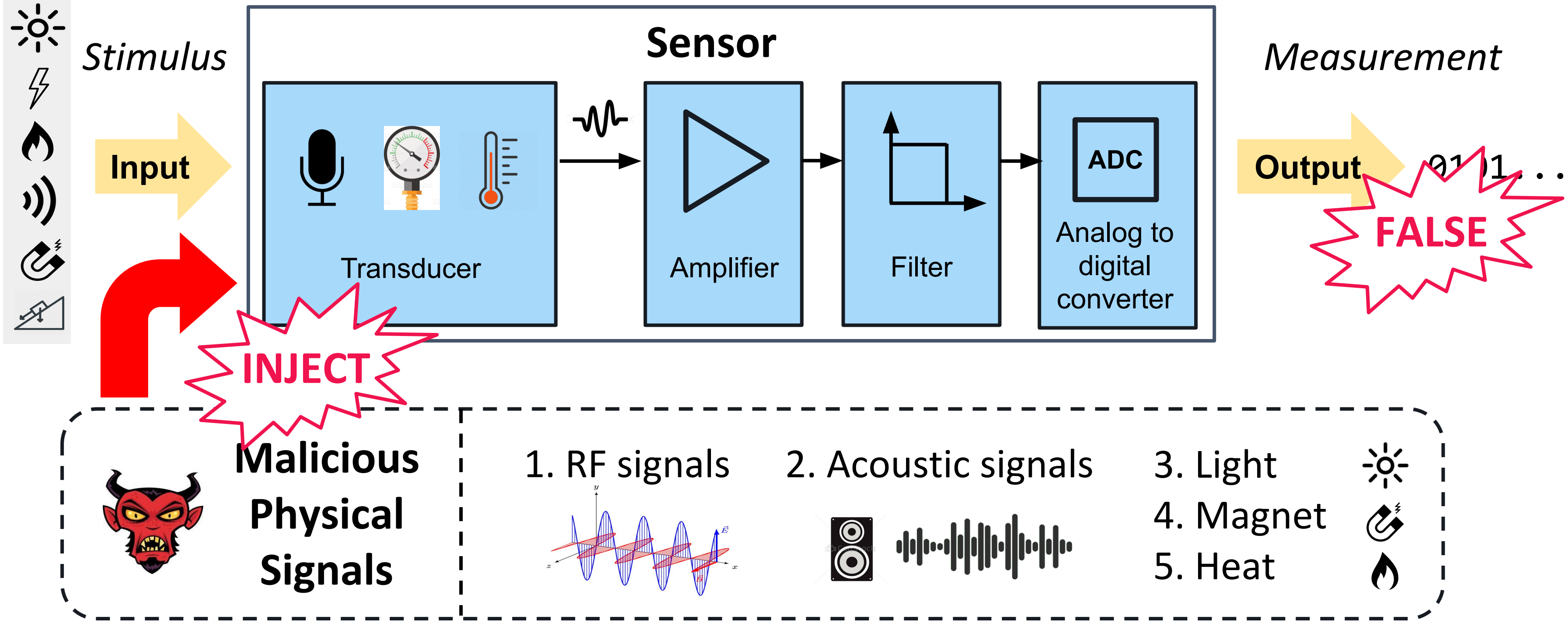
Contributions:

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?



How do transduction attacks work?



Simple Sensor Security Model

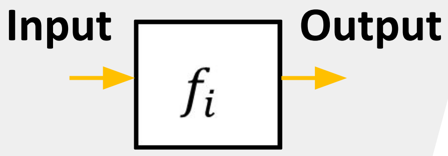
General Ideas

Common Properties

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

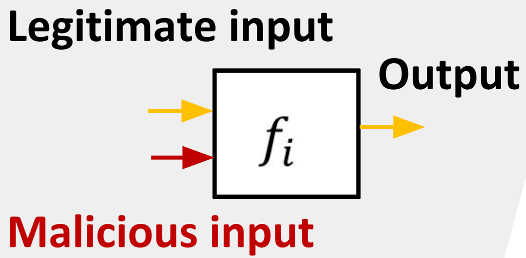
Sensor Model

Model each sensor component with a transfer function



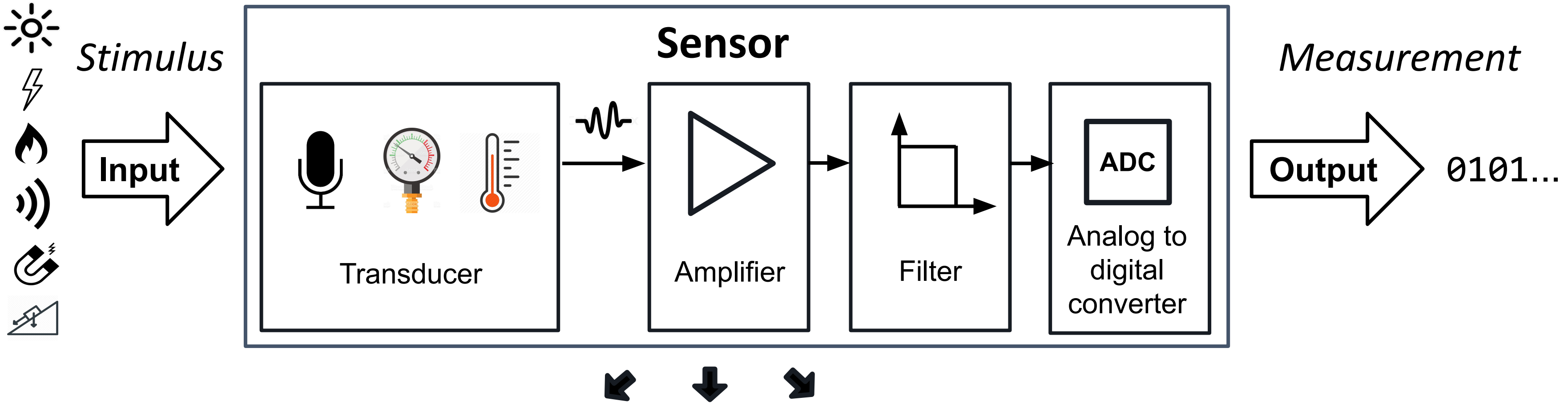
Adversary in the Model

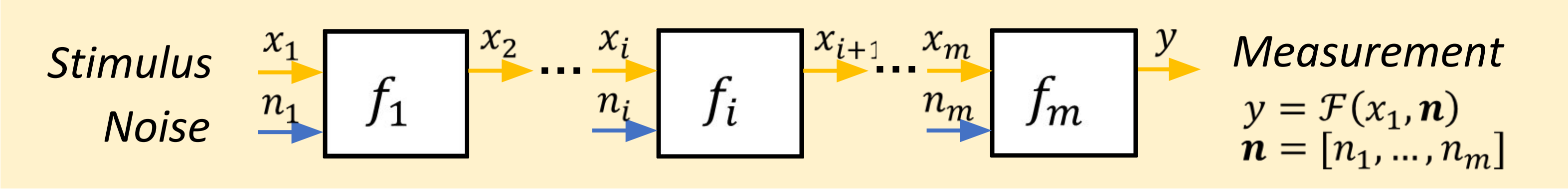
Model attacks by adding malicious signals into the model



Simple Sensor Security Model

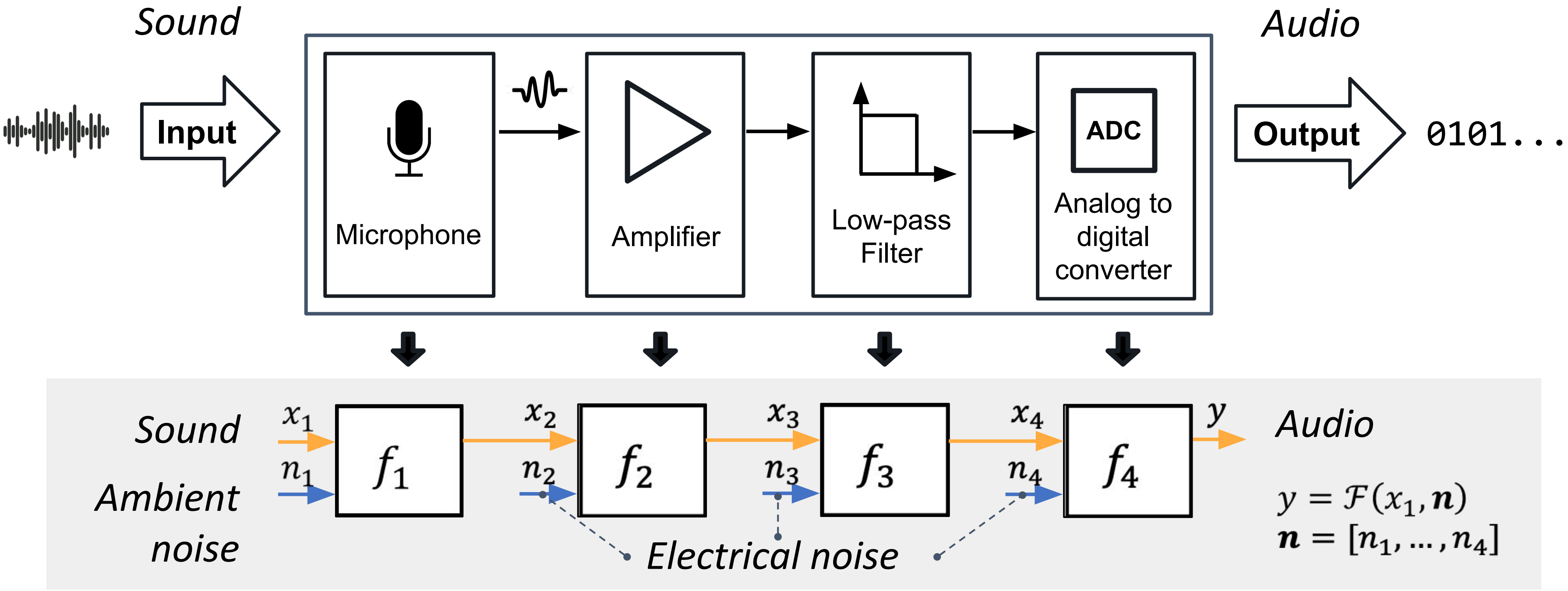
Transfer Function Representation





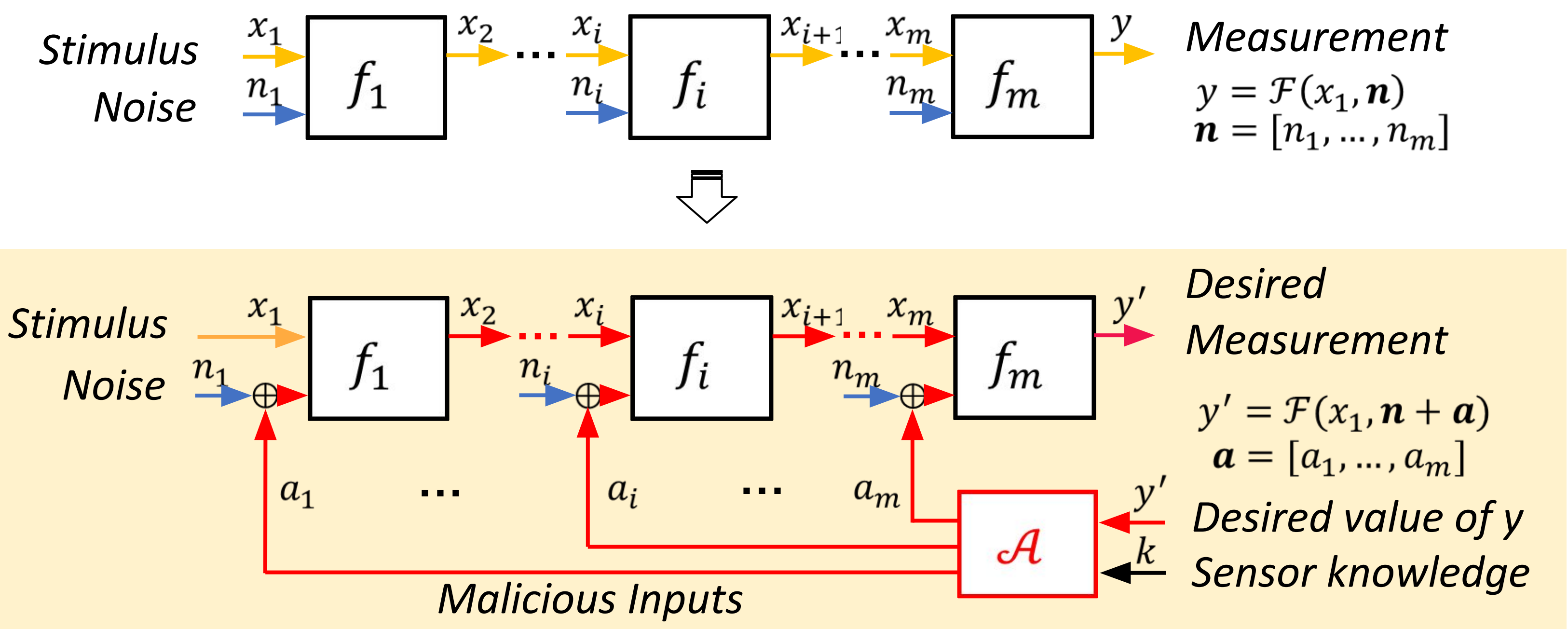
Simple Sensor Security Model

Transfer Function Representation: Microphone Example



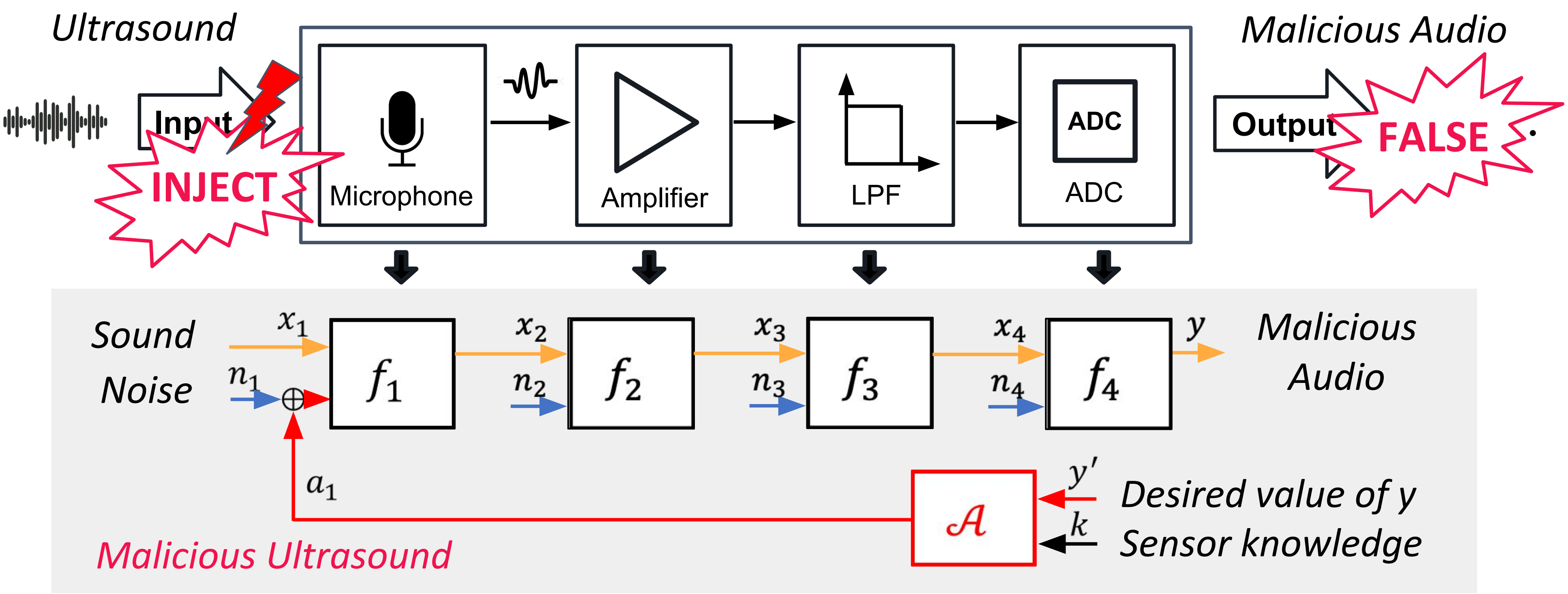
Simple Sensor Security Model

Adversaries in the Model



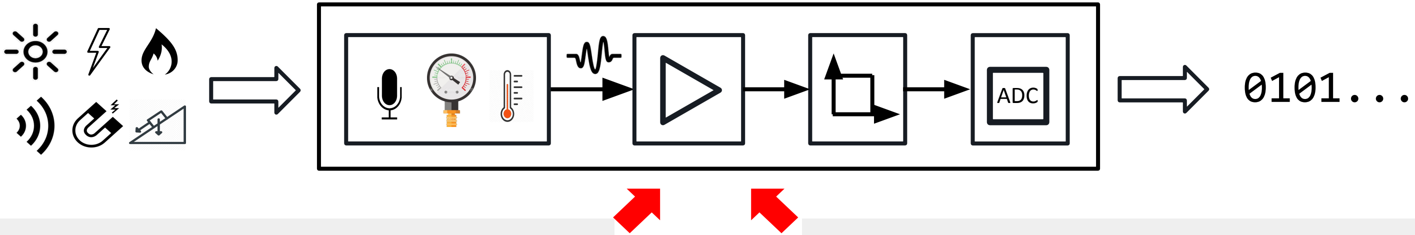
Simple Sensor Security Model

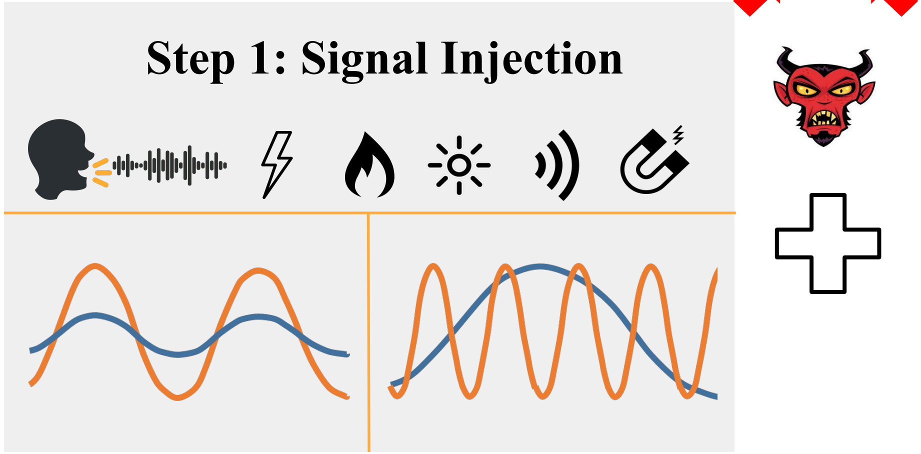
Example: DolphinAttack (*Zhang et al., CCS 2017*)

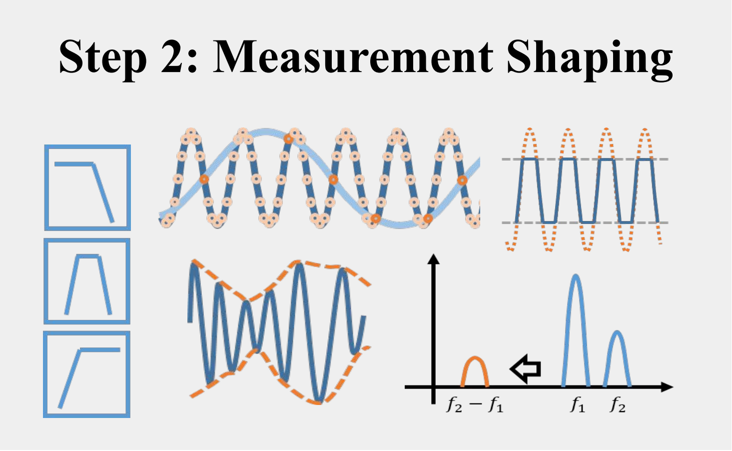


Attack Systemization

Common Attack Steps



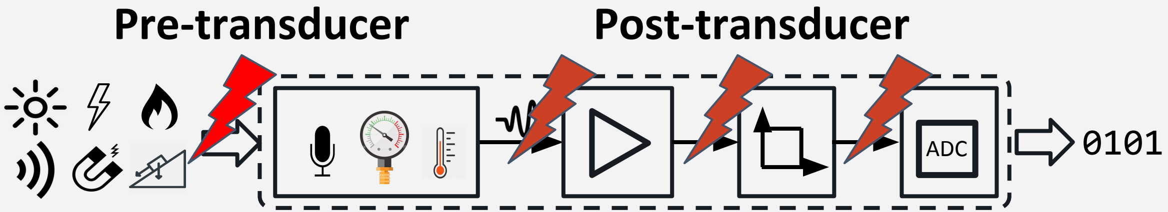




Attack Systemization

Signal Injection Step (3 factors)

Injection Point



Signal Type

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

Signal Frequency

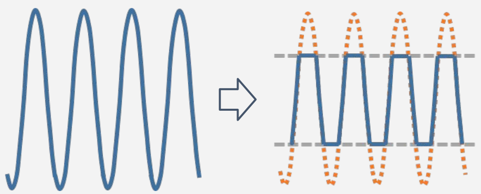
In-band vs. out-of-band

Sensor	Expected Operating Band	Attack Frequency
MEMS Inertial Sensor	≤ 750 Hz	> 1kHz
Microphone	≤ 20 kHz	> 20 kHz

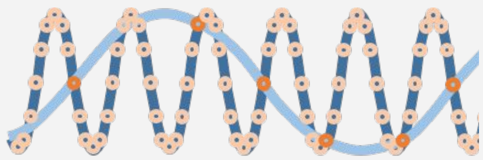
Attack Systemization

Measurement Shaping Step (5 types)

Saturation

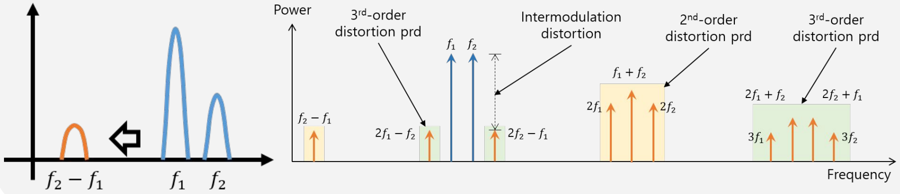


Aliasing

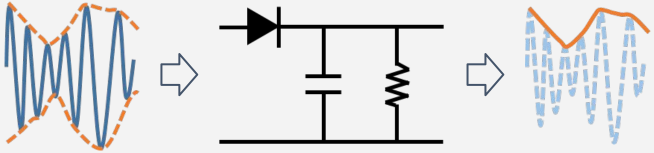


Filtering

Intermodulation Distortion

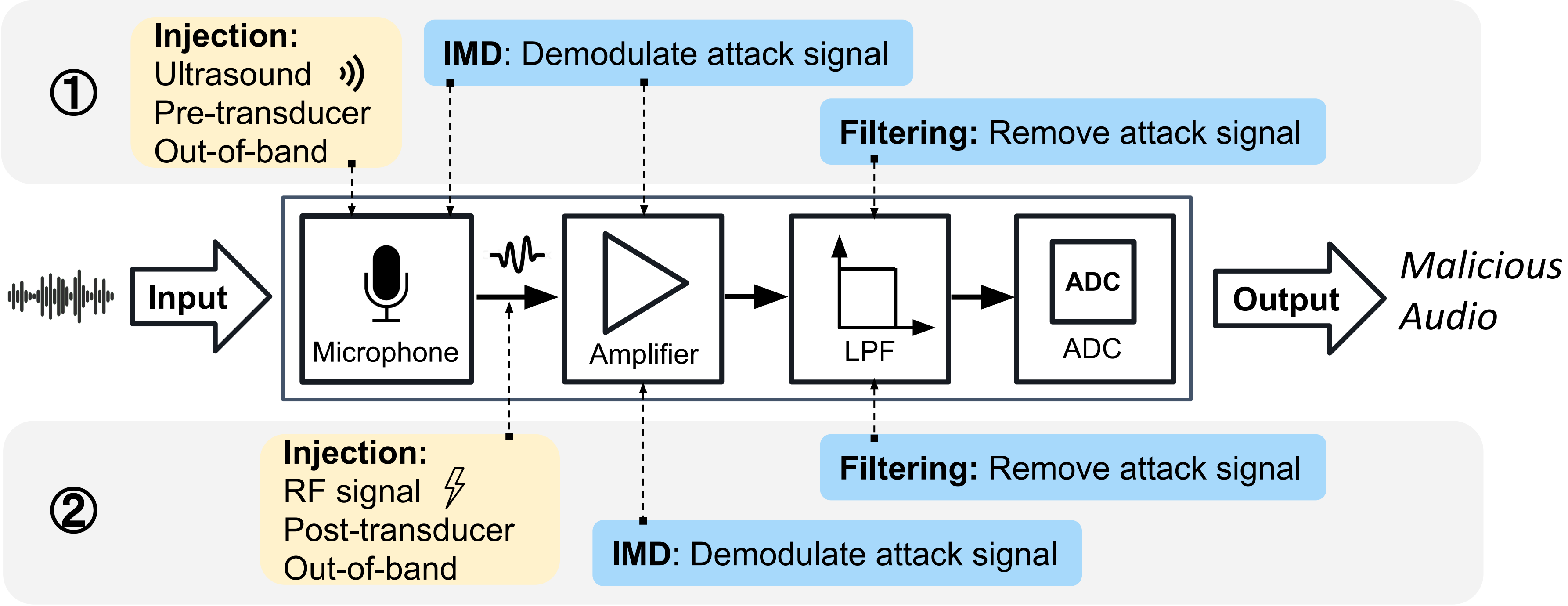


Envelope Detection



Attack Systemization

Example: ① DolphinAttack & ② Ghost Talk



Attack Systemization

Summary

TABLE II: SYSTEMATIZATION OF TRANSDUCTION ATTACKS WITH THE SIMPLE SENSOR SECURITY MODEL.

Sensor			Exploited Component					Signal Injection			Measurement Shaping					Outcome		Paper
Application	Type	C	Trans.	Wire	Amp.	Filter	ADC	Point	Type	Freq.	Sat.	IMD	Fil.	Env.	Ali.	DoS	Spoof	
Automobile	Lidar	A	●	○	◐	○	○	Pre	✷	In	●	○	○	○	○	●	○	[45]
											○	○	○	○	○	○	●	[45], [46]
	Camera	P	●	○	◐	○	○	Pre	✷	In	●	○	○	○	○	●	○	[46], [70]
	Radar	A	●	○	◐	○	○	Pre	📶	In	◐	○	○	○	○	●	○	[70]
											○	○	○	○	○	○	●	[70], [95]
	Ultrasonic Sensor	A	●	○	◐	○	○	Pre	🔊	In	◐	○	○	○	○	●	○	[68], [70]
											○	○	○	○	○	○	●	[68], [70]
	Magnetic Encoder	A	●	○	○	○	○	Pre	🧲	In	○	○	○	○	○	●	●	[96], [97]
S	Microphone	P	●	●	●	●	●				○	○	●	○	●	○	●	[47]
								Pre	🔊	Out	◐	●	○	○	○	●	○	[100]–[102]
											○	●	○	○	○	○	●	[80], [90]–[92]
	Touchscreen	A	●	○	○	◐	○	Pre	ϟ	N/A	○	○	◐	○	○	●	●	[103]
Hard Disk	MEMS Shock Sensor	P	●	○	◐	●	○	Pre	🔊	Out	◐	○	●	○	○	○	●	[86]
Energy	Infrared Sensor	P	○	●	○	◐	●	Post	📶	Out	●	○	◐	○	○	◐	◐	[75], [76]
Medical Devices	Pacemaker Lead Defibrillator Lead	P	○	●	○	○	○	Post	📶	In	○	○	○	○	○	○	●	[47]
	Drop Counter	A	●	○	◐	○	○	Pre	✷	In	●	○	○	○	○	●	●	[87]

✷ Visible light or infrared 📶 RF waves 🔊 Audible sound or ultrasound 🧲 Magnetic field ϟ Electric field ● Applicable ◐ Probable ○ Not applicable

C. Category **A** Active sensor **P** Passive sensor **Pre** Pre-transducer **Post** Post-transducer **In** In-band **Out** Out-of-band **N/A** Not available

Sensor Categories

Exploited Component

Signal Inject Steps

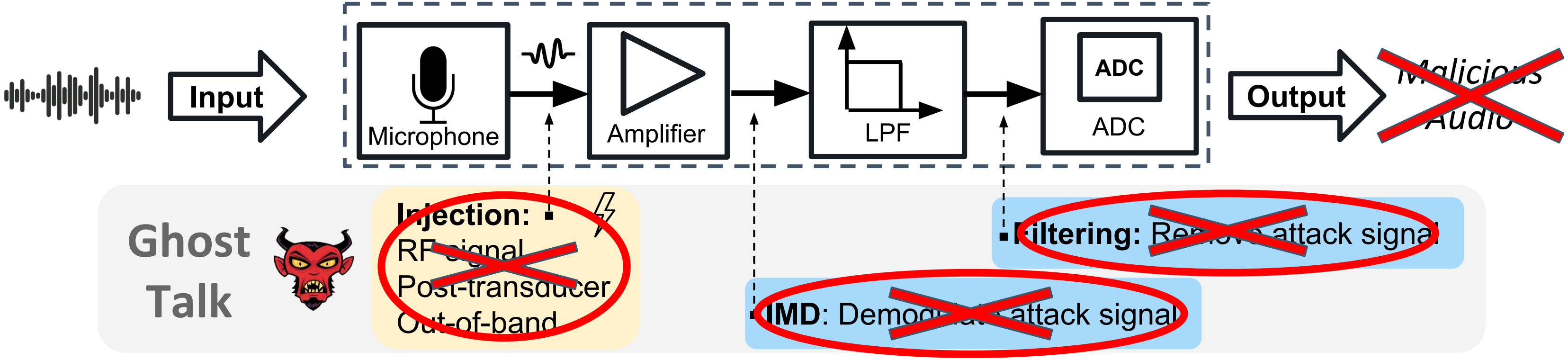
Measurement Shaping Steps

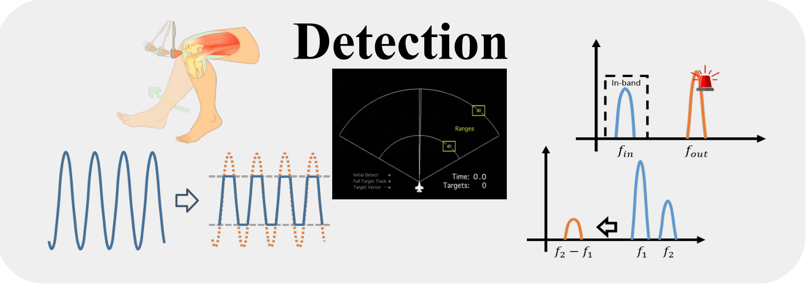
Outcome

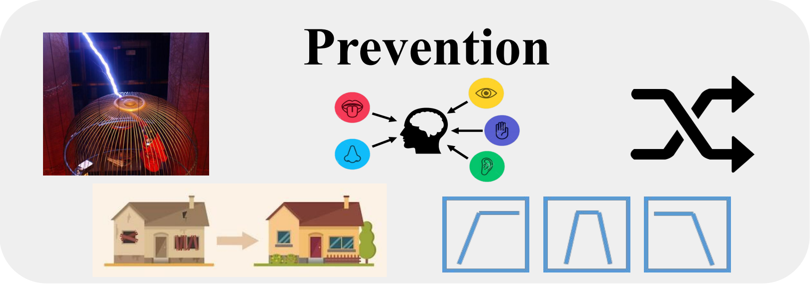
Paper

Defense Systemization

Detection and Prevention





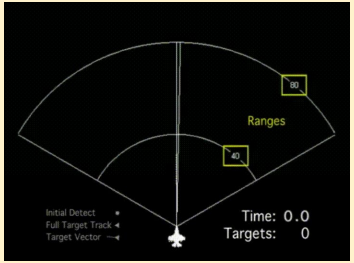


Defense Systematization:

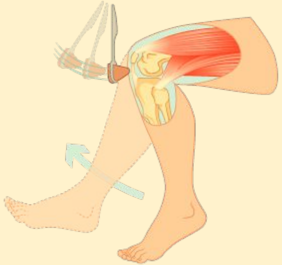
Detection

Injection

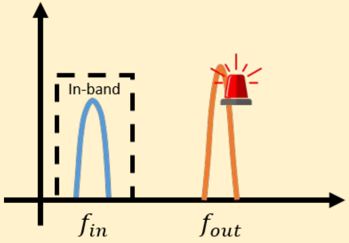
TX Randomization



Verifying Actuation

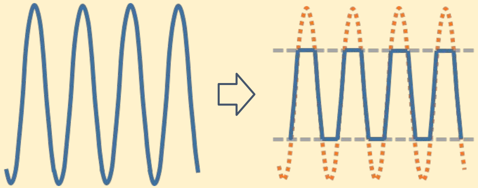


Detecting Out-of-band

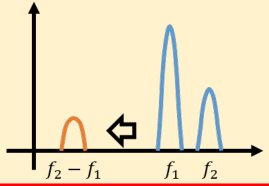


Measurement Shaping

Saturation Detection

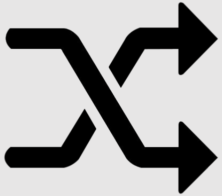


IMD Feature Detection

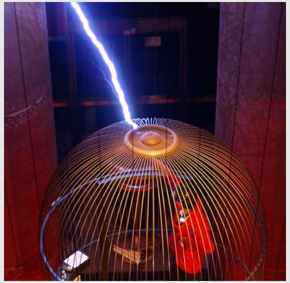


Defense Systematization:
Prevention

Randomization

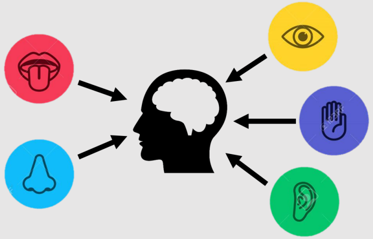


Shielding



Filtering

Fusion



Component Quality Improvement

Defense systematization

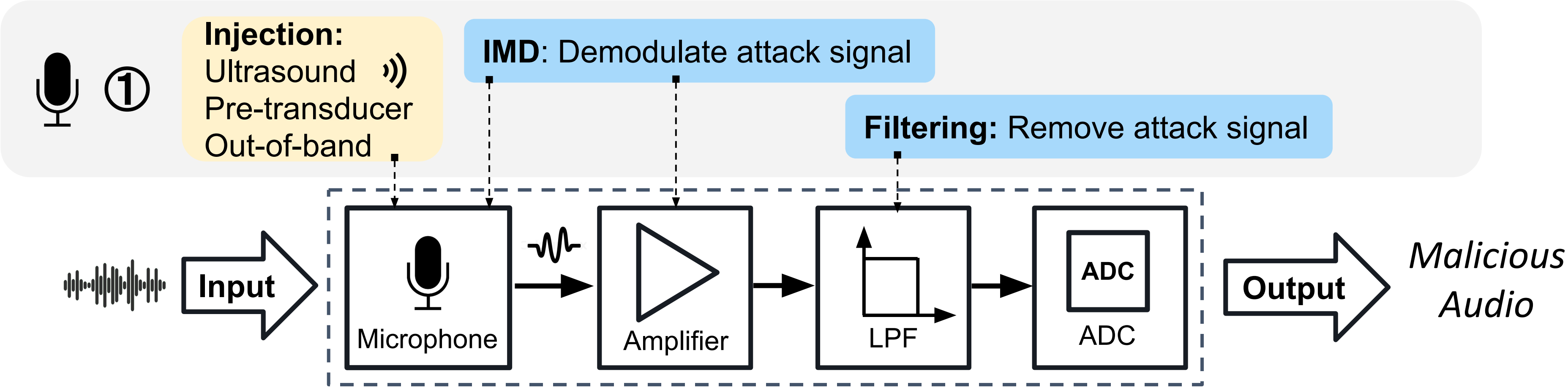
TABLE III: SYSTEMATIZATION OF TRANSDUCTION ATTACK DEFENSES

Goal	Cat.	Subcat.	Related Component							Injection and Shaping Steps							Xfer[1] Func.	Paper
			TX	Trans.	Wire	Amp.	Fil.	ADC	Dig.[2]	Point	Freq.	Sat.	IMD	Fil.	Env.	Ali.		
ection	Inject.	TX randomiz.	●	○	○	○	○	○	●	Both	Both	○	○	○	○	○	N/A	[68], [87], [106]
		Verif. Actuation	●	○	○	○	○	○	●	Both	Both	○	○	○	○	○		[47], [107]
		Detect OOB Sig.	○	●	○	○	○	○	●	Pre	Out	○	○	○	○	○		[44], [86]
Goal	Category and Subcategory		Related Component(s)							Injection and Shaping Steps							Xfer Function	Paper
	Fusion	Spatial Fusion	●	●	●	●	●	●	●	Steps differ case by case							P3	[44], [45], [68], [70], [86]
		Spectral Fusion	●	●	○	○	○	○	●								P1,P3	[46]
		Temporal Fusion	○	○	○	○	○	○	●								P1	[46], [68], [98]
	Comp. Quality Improv.		●	●	●	●	●	●	○								P1	[42], [44], [59]

[1] Denotes the three xfer func. models of Section V-B. [2] Digital Backend [3] Attack Surface Reduction ● Applicable ○ Not applicable

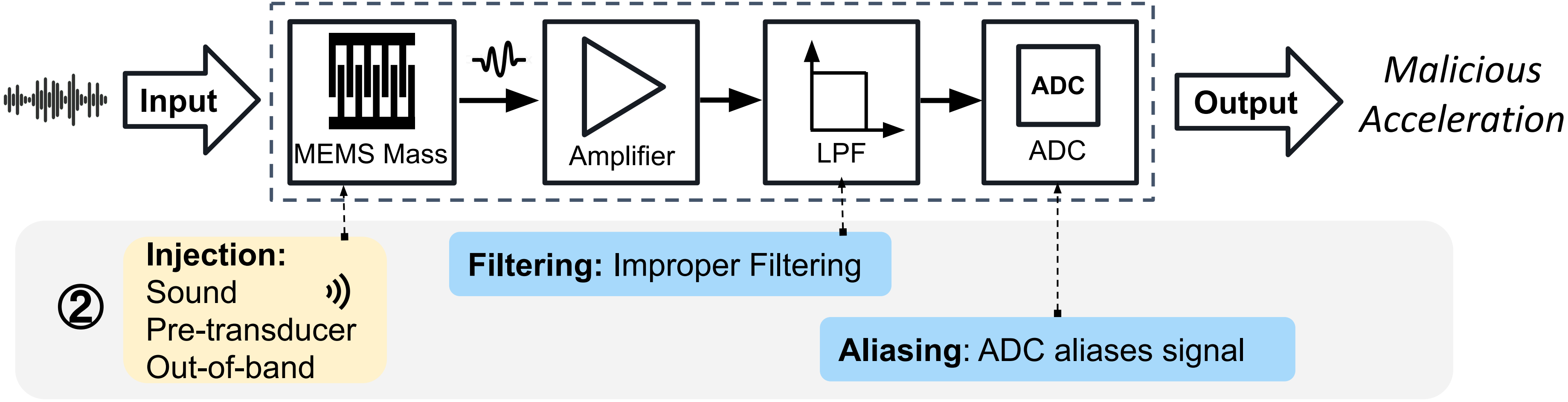
Prediction: Attacks

Example: Part ① DolphinAttack



Prediction: Attacks

Example: Part ② Walnut



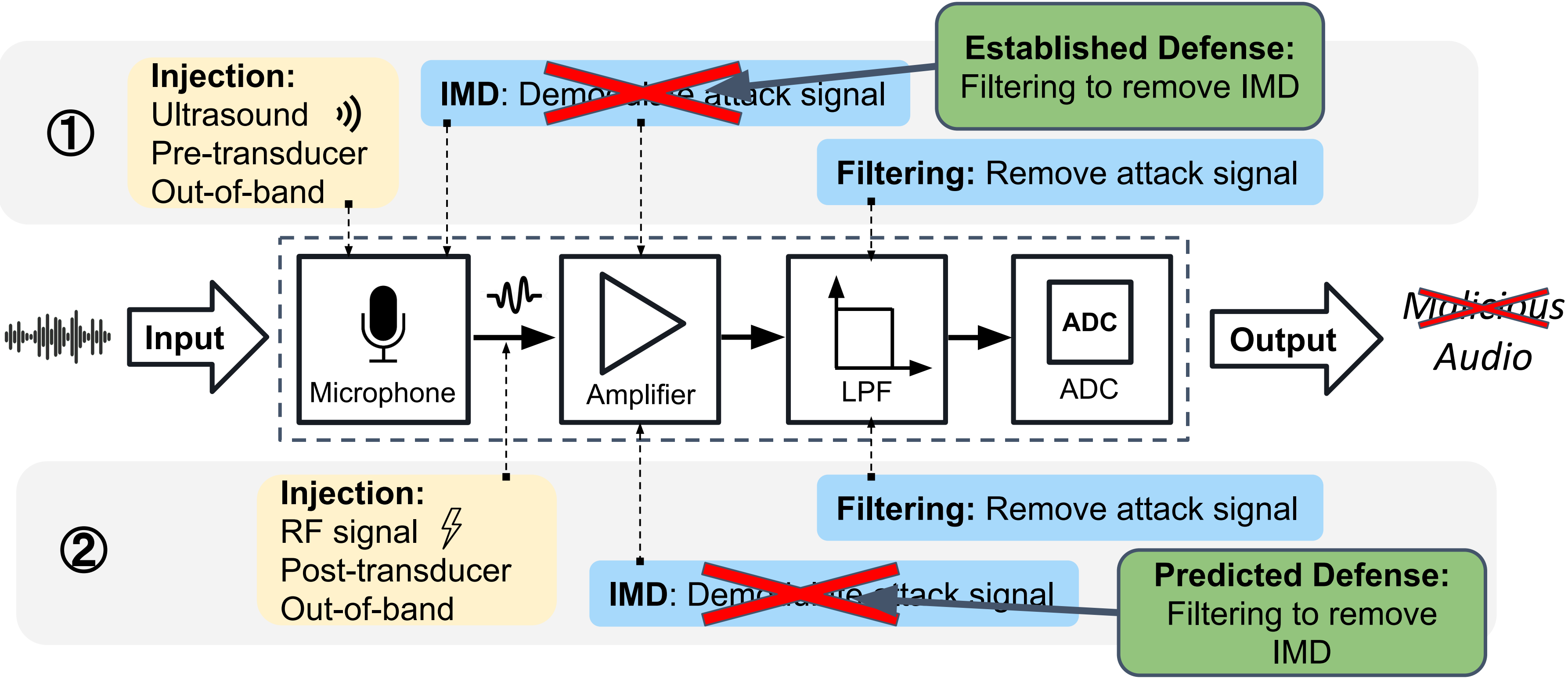
Prediction: Attacks

Example: Part ③ predicting an attack

	AM Injection	Attacker Methods for AM Demodulation	
①	**Injection:** Ultrasound Pre-transducer Out-of-band	**IMD**: Demodulate attack signal	**Filtering:** Remove attack signal
②	**Injection:** Ultrasound Pre-transducer Out-of-band	**Filtering:** Improper Filtering	**Aliasing**: ADC aliases signal
Predict	**Injection:** Ultrasound Pre-transducer Out-of-band	**Filtering:** Improper Filtering	**Aliasing**: ADC aliases signal

Prediction: Defenses

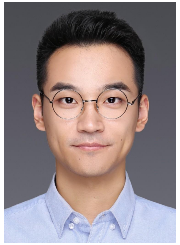
Example: ① DolphinAttack & ② Ghost Talk



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






Chen Yan, Hocheol Shin, Connor Bolton,
Wenyuan Xu, Yongdae Kim, Kevin Fu

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/hocheolshincv
cyans.cn

We thank our shepherd Prof. Brendan Dolan-Gavit 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.