浙江大學
ZHEJIANG UNIVERSITY

Rethinking IoT Security: Understanding and Mitigating Out-of-Band Vulnerabilities

冀晓宇

2023年10月26日

智能系统安全实验室
UBIQUITOUS SYSTEM SECURITY LAB.

Internet vs. Internet of Things

Internet

VS

IoT

- Connecting **people**
- Connecting the **virtual** world

- Connecting **everything**
- Connecting the **physical** world

History of IoT

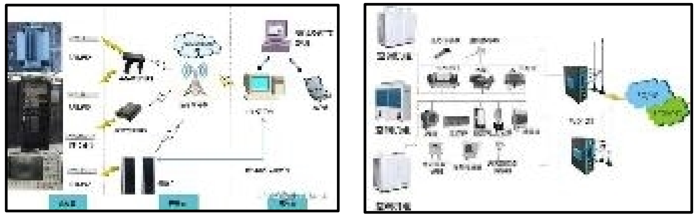
I: Nascent Stage

Connecting vending machines and coffee machines

“Point-2-Point Sensing”

1980s-1990s

II: Connectivity



RFID + Networked sensing systems

“Networked Sensing”

Early 21st century

III: Intelligence

Autonomous systems that can make decision without human intervention.

“Sensing and Control”

2010s-present

The Beginning of IoT Devices

1982: CMU's
Coke machine

1990: John Romkey's
"Internet Toaster"

2000: LG's
Internet refrigerator

Stage II: Weirdest IoT Enabled Devices

Who’s the most proficient crapper in your office

@jsheldrick:
My heart has just stopped.
Goodbye to all my followers,
I loved you all. #finalfarewell

BeatTweeter. The ring that sends condolences to your nearest and dearest when your heartbeat stops.

Stage III: Intelligence Stage: Sensing + Control + AI

- **Autonomous Systems (AS) are capable of performing tasks or operations without direct human intervention.**

Unmanned vehicles

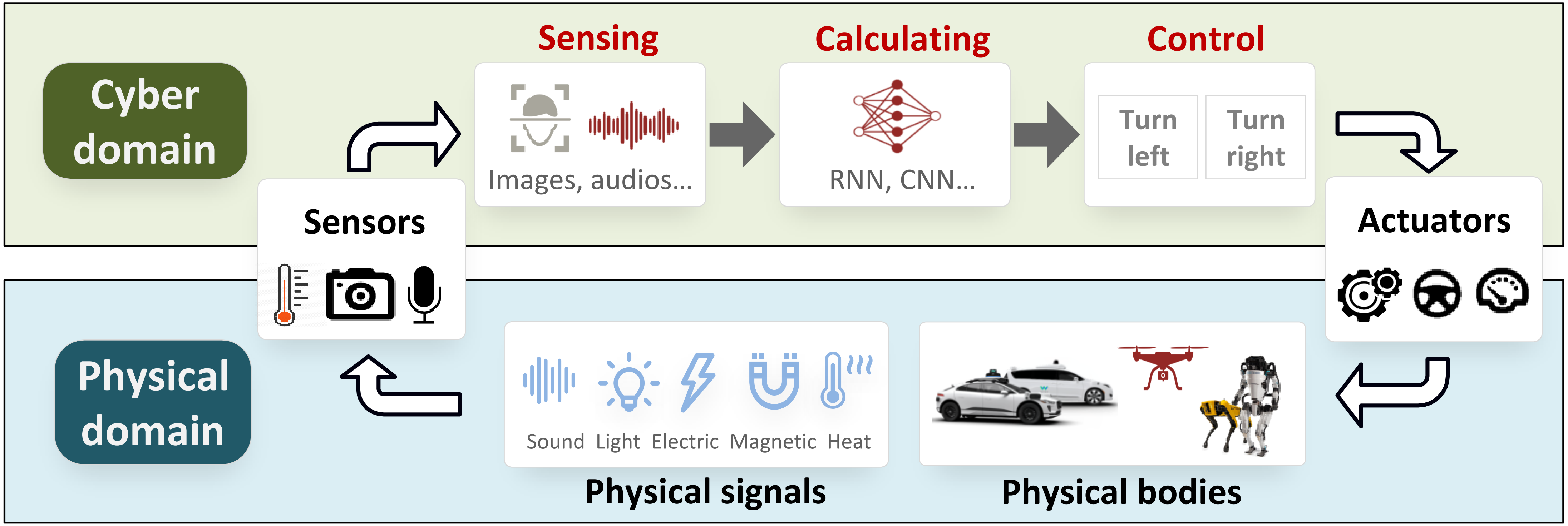
Drones

Robots

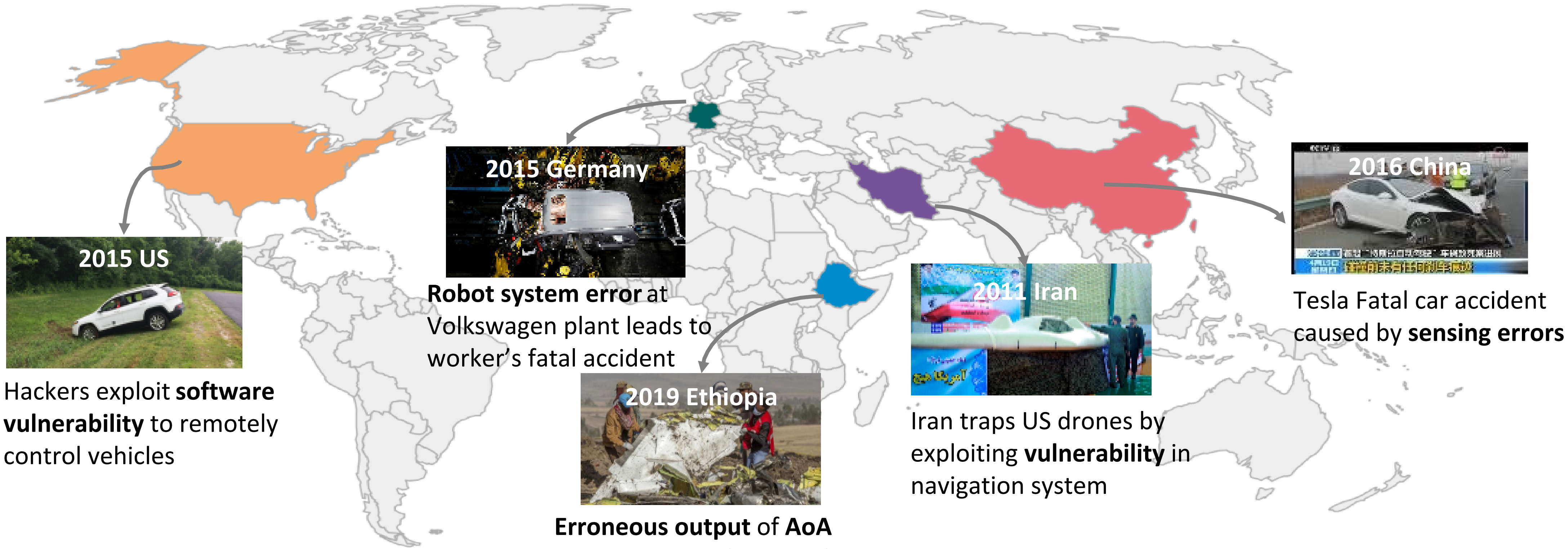
…

Autonomous Systems

- Sensing → Calculating (AI) → Actuating
- Cross-domain interactions between the physical domain and cyber domain



Security Accidents of AS



Hackers exploit **software vulnerability** to remotely control vehicles

Robot system error at Volkswagen plant leads to worker’s fatal accident

Erroneous output of **AoA sensor** causes plane crashes

Iran traps US drones by exploiting **vulnerability** in navigation system

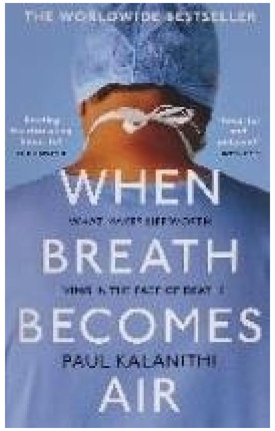
Tesla Fatal car accident caused by **sensing errors**

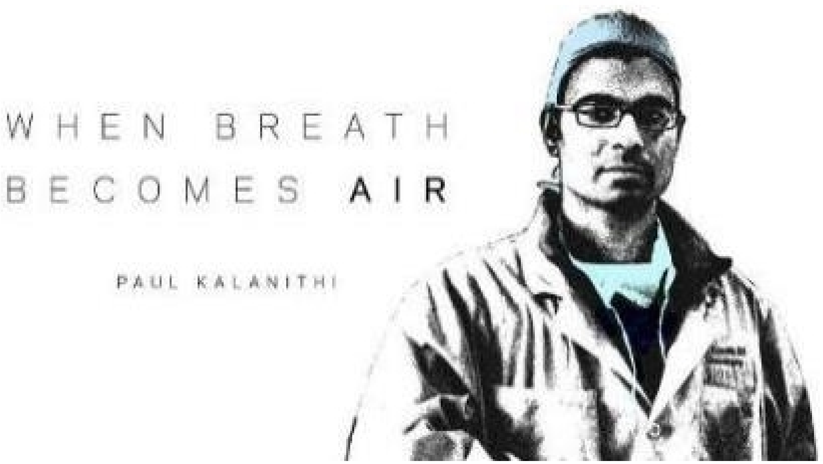
The root cause of security accidents of vehicles is **vulnerabilities.**

How to explore IoT-specific vulnerabilities?

You that seek what life is in death,
Now find it air that once was breath.
New names unknown, old names gone:
Till time end bodies, but souls none.
Reader! then make time, while you be,
But steps to your eternity.

——by Baron Brooke Fulke Greville





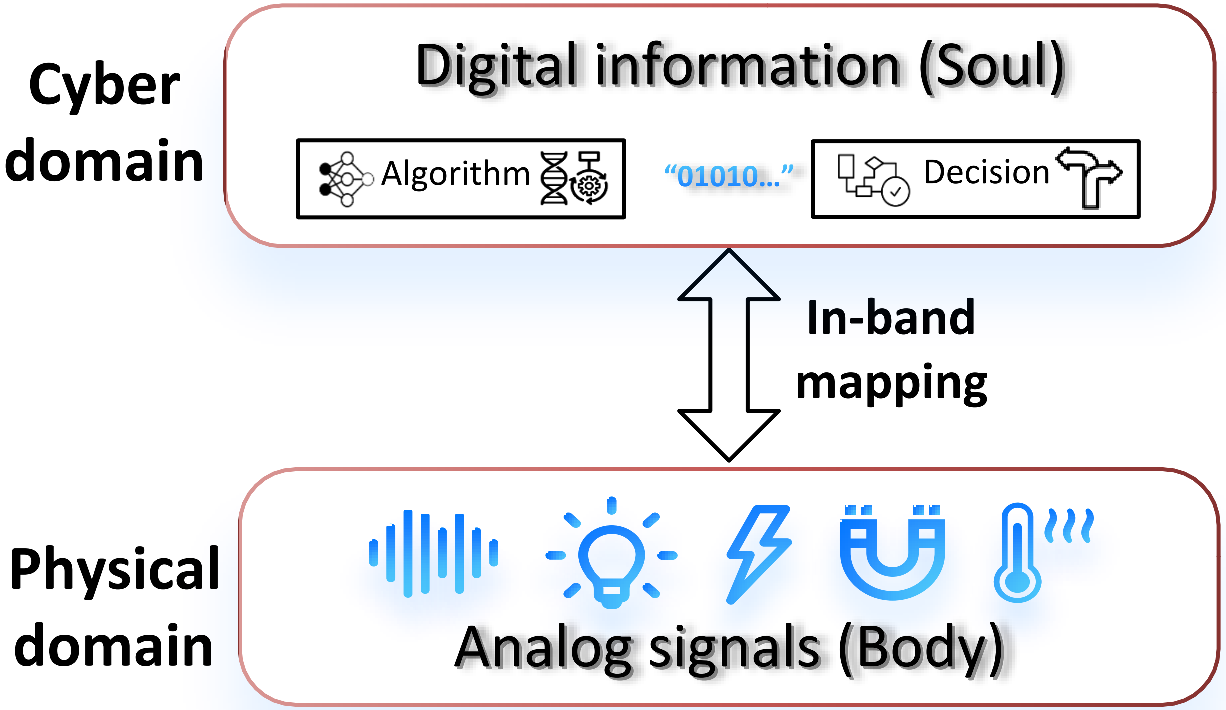
Inspiration of Life: Body or Soul?

The mind was simply the operation of the brain.

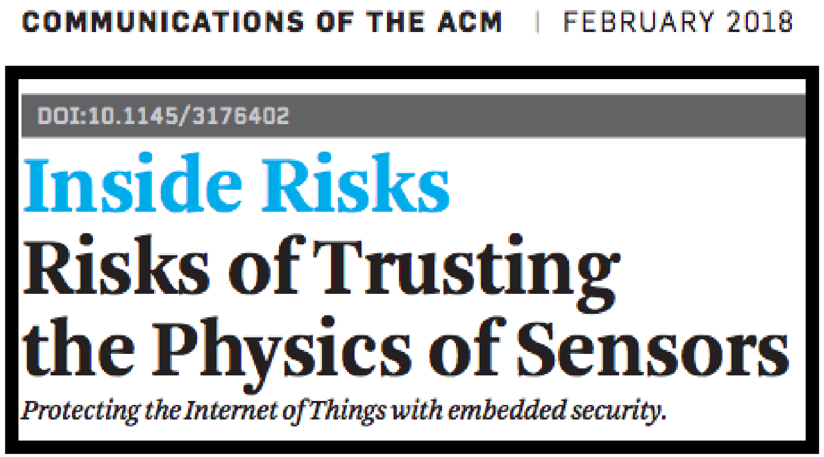
Body and Soul of IoT

Does IoT have body and soul?

The digital bits were simply the operation of the analog signals



Soul is Doomed with a Flawed Body



COMMUNICATIONS OF THE ACM | FEBRUARY 2018

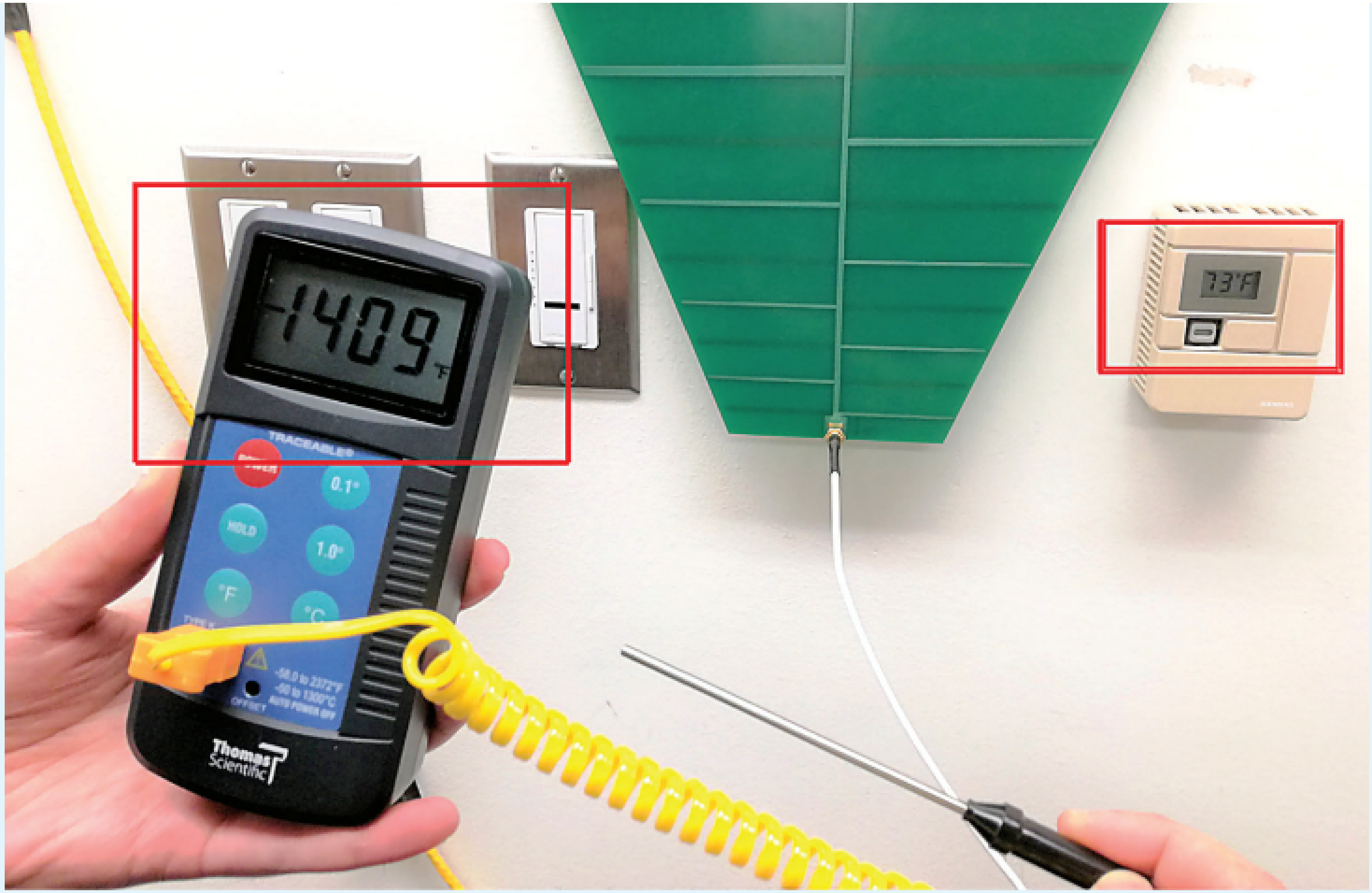
DOI:10.1145/3176402

Inside Risks

Risks of Trusting the Physics of Sensors

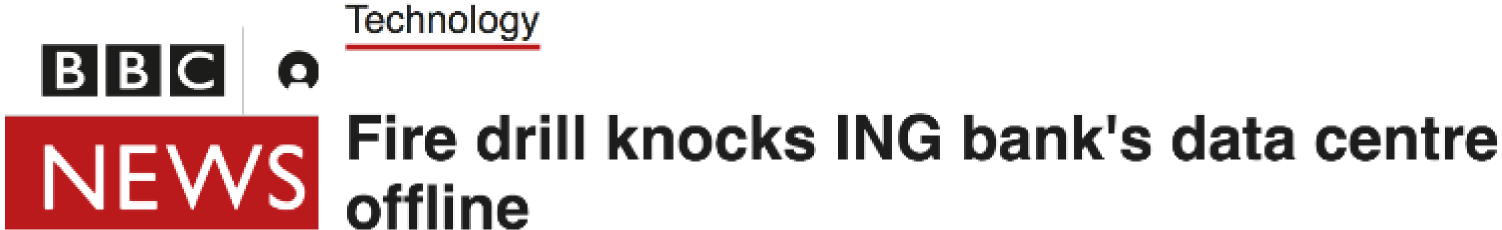
Protecting the Internet of Things with embedded security.

- **Physical signals directly affect thermocouple thermometers**
  - Thermocouples measure voltage to infer temperature
  - It is not always the temperature that induces the voltage



Sensor Vulnerability

Soul is Doomed with a Flawed Body



BBC NEWS

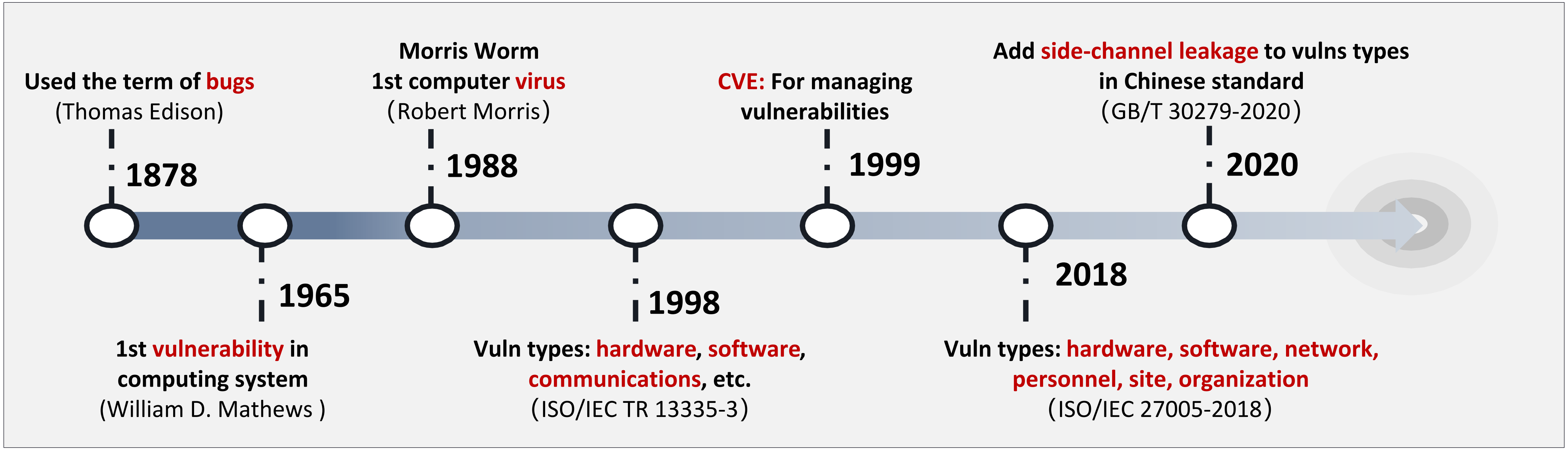
Technology

Fire drill knocks ING bank's data centre offline

Why?

The History of Vulnerabilities

- A vulnerability is a flaw in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. ---[IETF RFC 4949]



1878
Used the term of bugs
(Thomas Edison)

1965
1st vulnerability in computing system
(William D. Mathews)

1988
Morris Worm
1st computer virus
(Robert Morris)

1998
Vuln types: hardware, software, communications, etc.
(ISO/IEC TR 13335-3)

1999
CVE: For managing vulnerabilities

2018
Vuln types: hardware, software, network, personnel, site, organization
(ISO/IEC 27005-2018)

2020
Add side-channel leakage to vulns types in Chinese standard
(GB/T 30279-2020)

ISO IEC CVE GB

Standard organizations

ModelSim OSSEC netsparker acunetix

Vulnerability detection tools

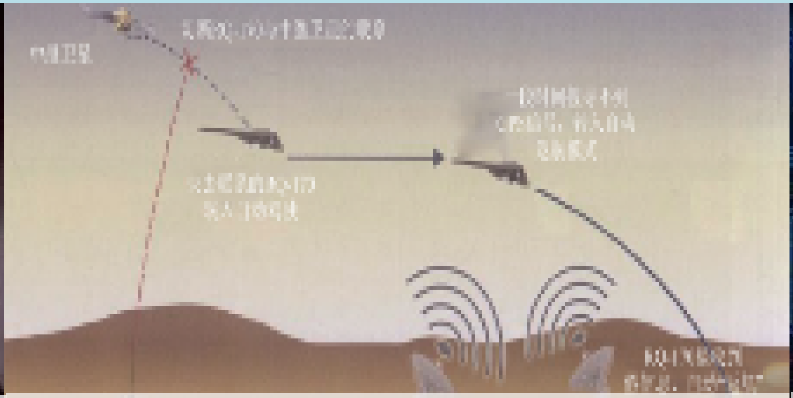
Vulnerability Taxonomy

Traditional Vulnerabilities

Hardware	Software	Network
Protocol	Physical Site	Organization

Vulnerabilities due to **function design** or implementation in one domain

Ransomware: exploits software vulnerabilities in OS to spread



Iran exploits protocol vulnerabilities in navigation systems to catch US drones

Meltdown: exploits hardware vulnerability in CPU to access sensitive information

Can existing vulnerability taxonomy cover IoT?

Transition from In-Band to Out-of-Band

- **What's missing? Vulnerabilities caused by abnormal cross-domain interaction**

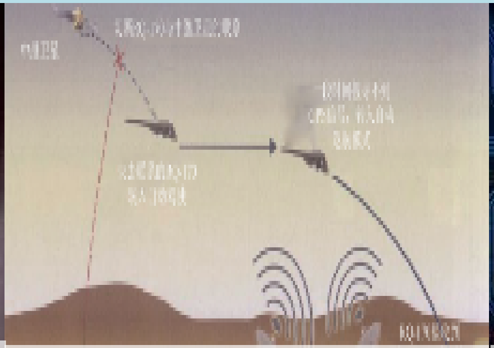
In-Band Vulnerabilities (Traditional)

Hardware | Software | Network

Protocol | Phy Site | Organization

Vuln. due to **function design** or implementation

Ransomware: exploits **software vulnerabilities** in OS to spread



Iran exploits **protocol vulnerabilities** to catch US drones

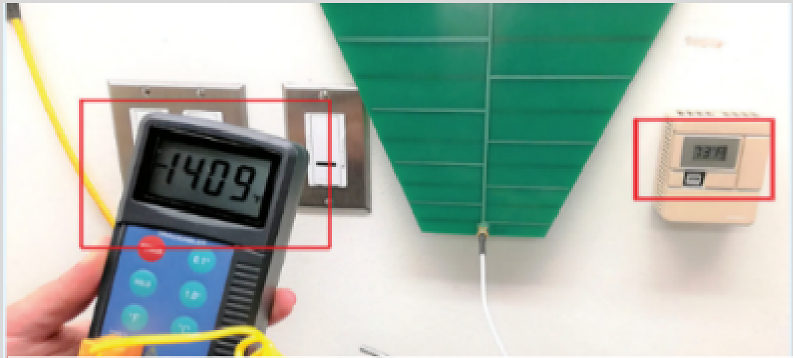
Meltdown: exploits **hardware vulnerability** in CPU to access information

Out-of-Band Vulnerability

Out-of-Range | Adversary Input

Cross-Sensing | Side Channel

Due to **abnormal cross-domain interaction**



Tampering thermocouple thermometer readings via electromagnetic waves

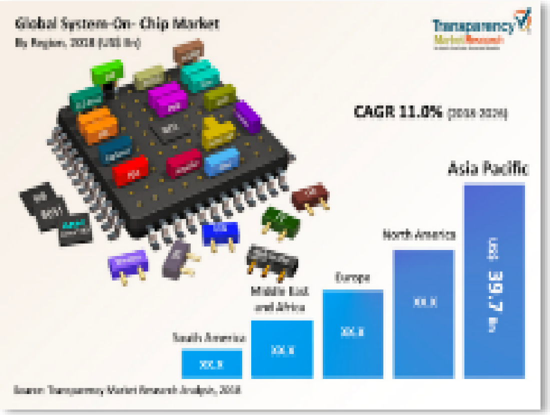
New Trends Create Out-of-Band Vulnerability

- **New trends in the autonomous system → Out-of-band vulnerabilities.**

Functional Complexity

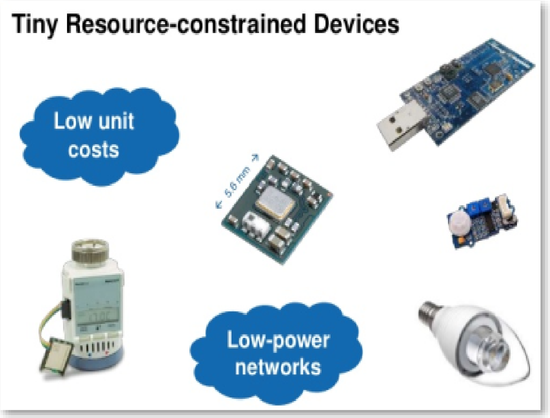
Device Miniaturization

System Integration

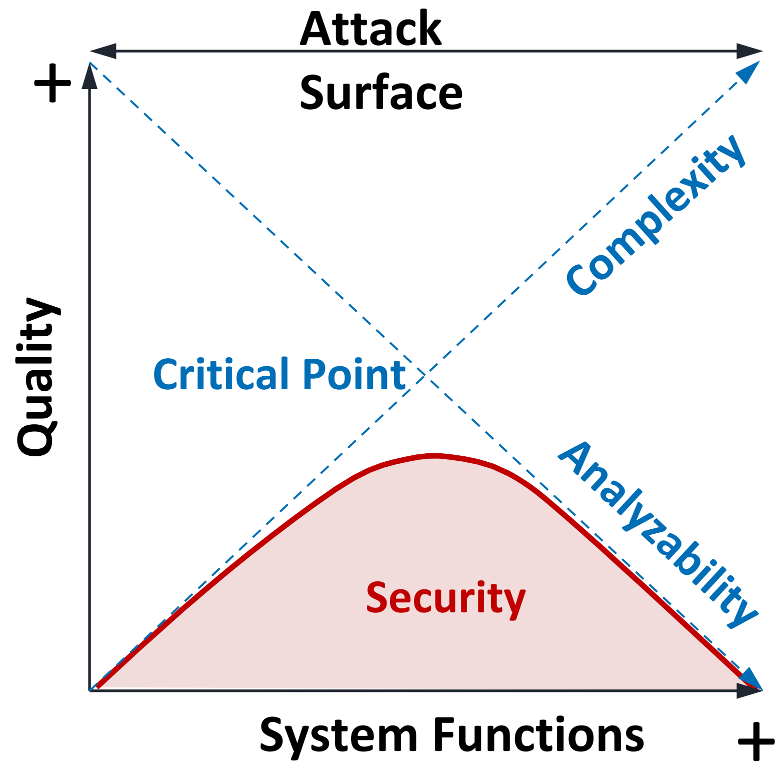


Source: Transparency Market Research Analysis, 2018

Resource Constraints



Functional Complexity



Software Security vs Complexity

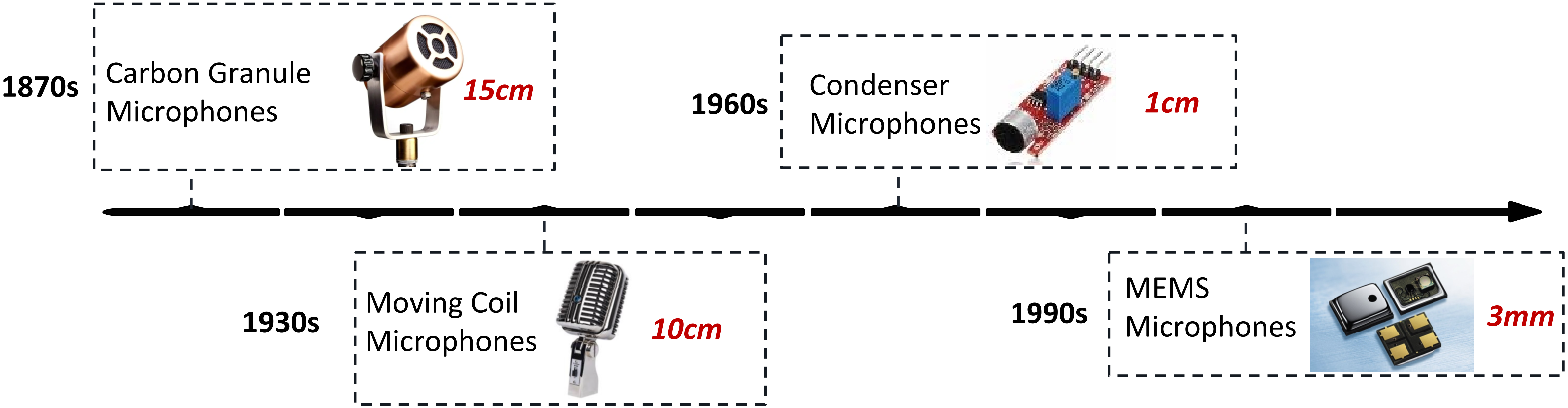
The more complex,

the less secure!

Alenezi, Mamdouh , and M. Zarour . "On the Relationship between Software Complexity and Security." *International Journal of Software Engineering and its Applications.*

Device Miniaturization

Miniaturisation of microphones creates greater out-of-band vulnerabilites



1870s Carbon Granule Microphones *15cm*

1930s Moving Coil Microphones *10cm*

1960s Condenser Microphones *1cm*

1990s MEMS Microphones *3mm*

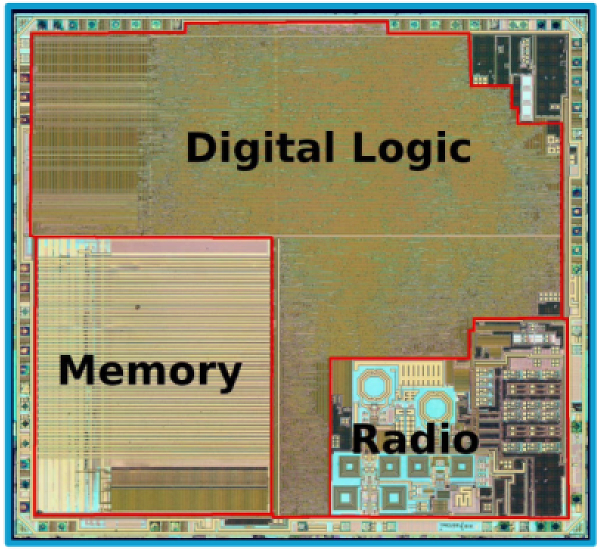
- Nonlinearity ⇨ ***Dolphin Attack***
- Photoacoustic effect ⇨ ***Light Command***

System Integration

- Logic Chip + Wireless Capabilities ⇨ ***Screaming Channel***

Mixed-signal chip

Encryption algorithm AES-128

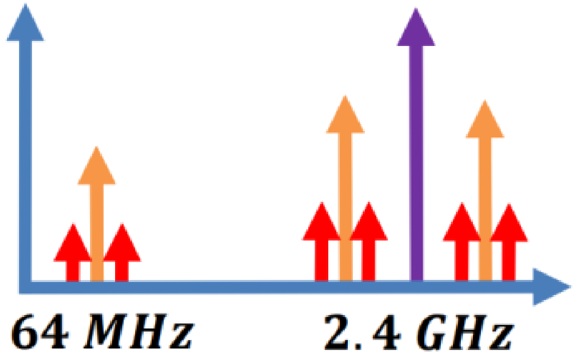


Bluetooth RF signal

Encryption information coupled via substrate

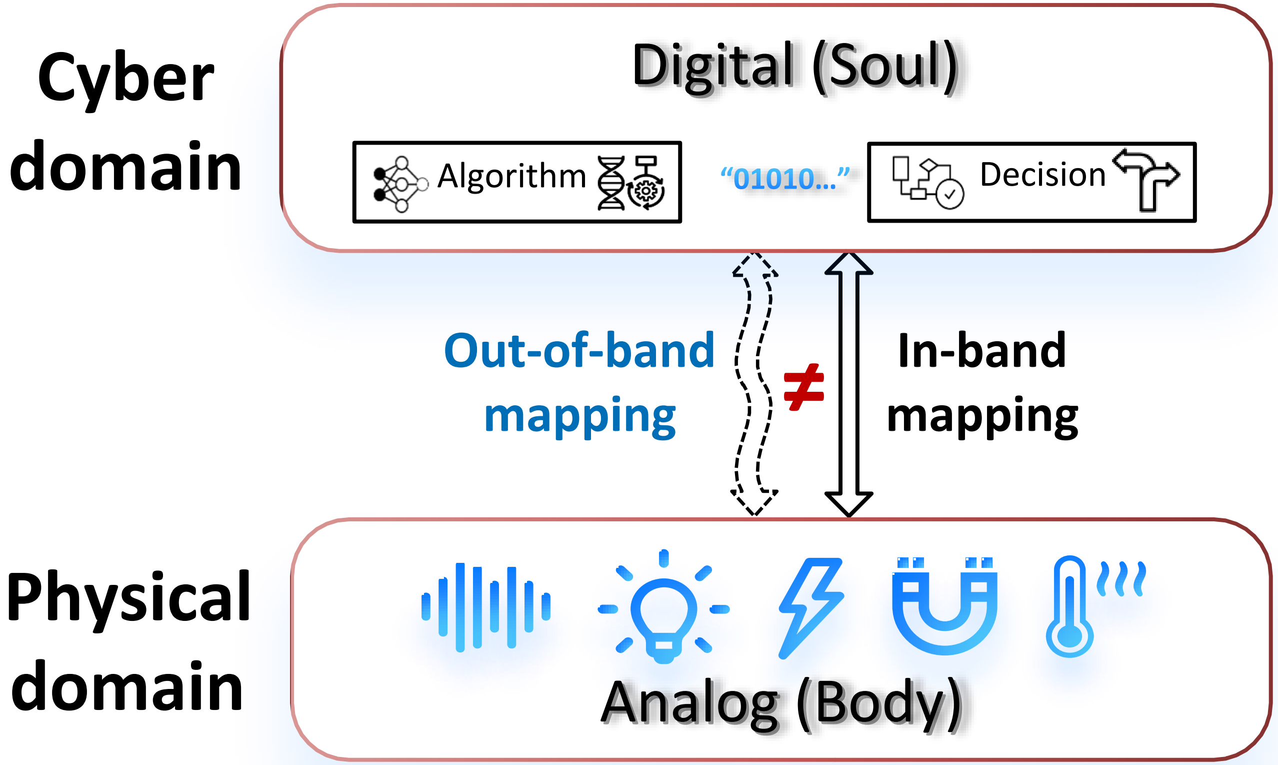
Conventional Side Channel Leak

Leak Propagation



Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," CCS '18.

In-Band Vulnerability vs. Out-of-Band Vulnerability



In-band vulnerability: weaknesses due to functional design or implementation flaws in a **single domain**

Out-of-band vulnerability: weaknesses due to non-functional design flaws during interactions **between domains**

Out-of-Band Vulnerability Types

Out-of-Range

Signal out of design range
Causes distortion of information output

Cross-Sensing

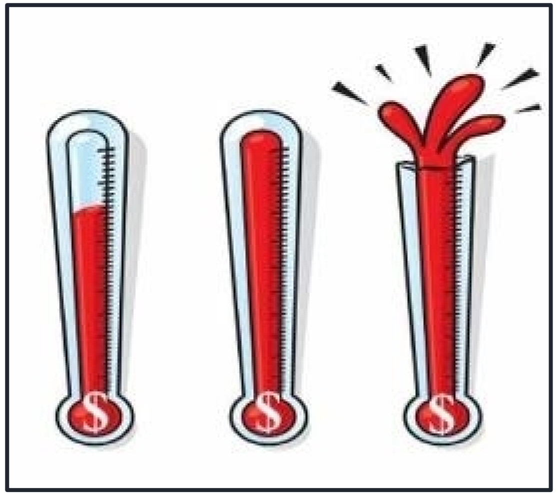
Senses cross-field signals
Causes abnormal back-end information

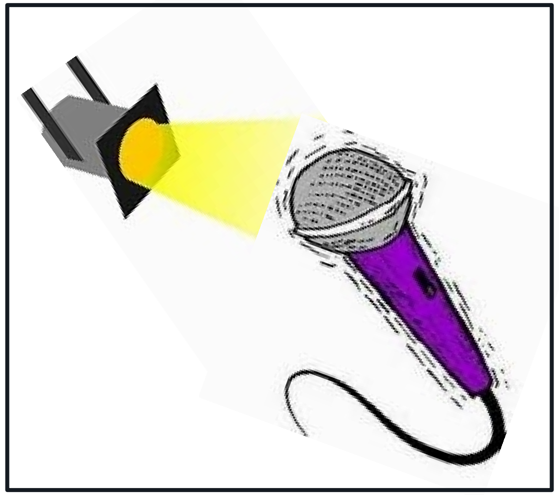
Adversary Input

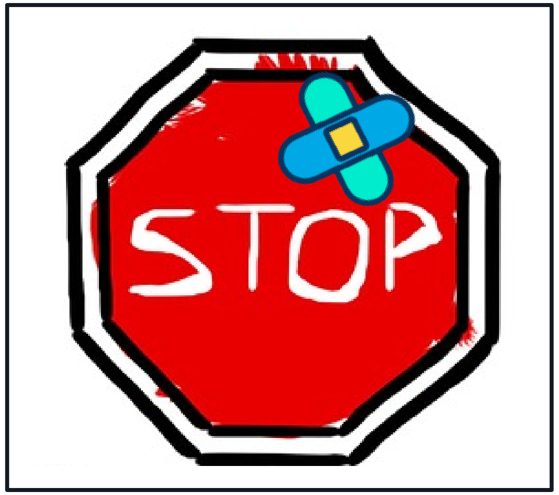
Specific physical inputs
Causes recognition errors

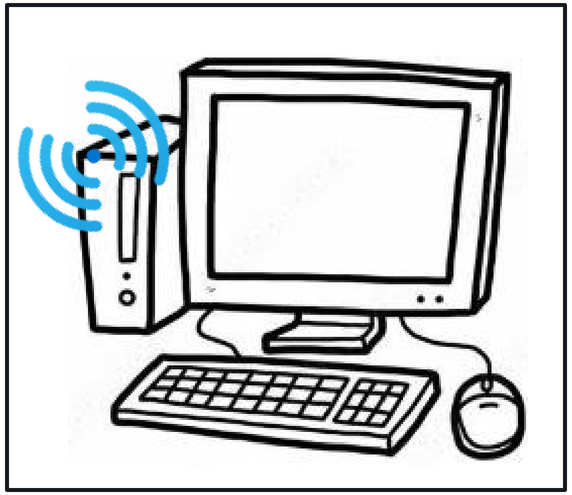
Side Channel

Side channel radiation in calculating
Causes system information leakage



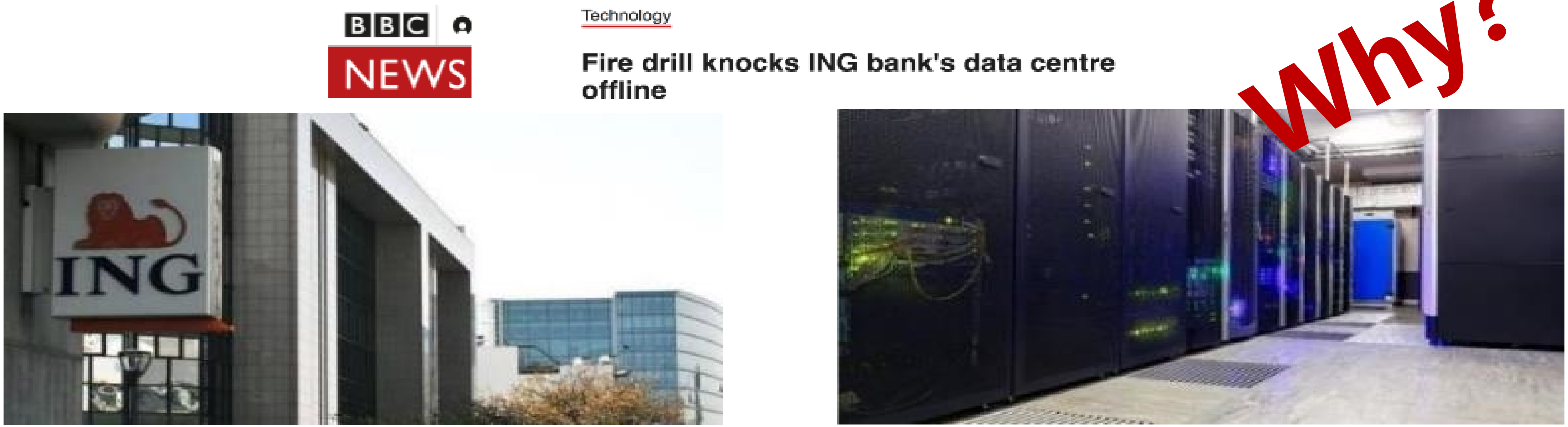






1. Out-of-Range

Root causes: the amplitude, shape, frequency of the signal is outside the expected range, resulting in unexpected consequences



BBC NEWS

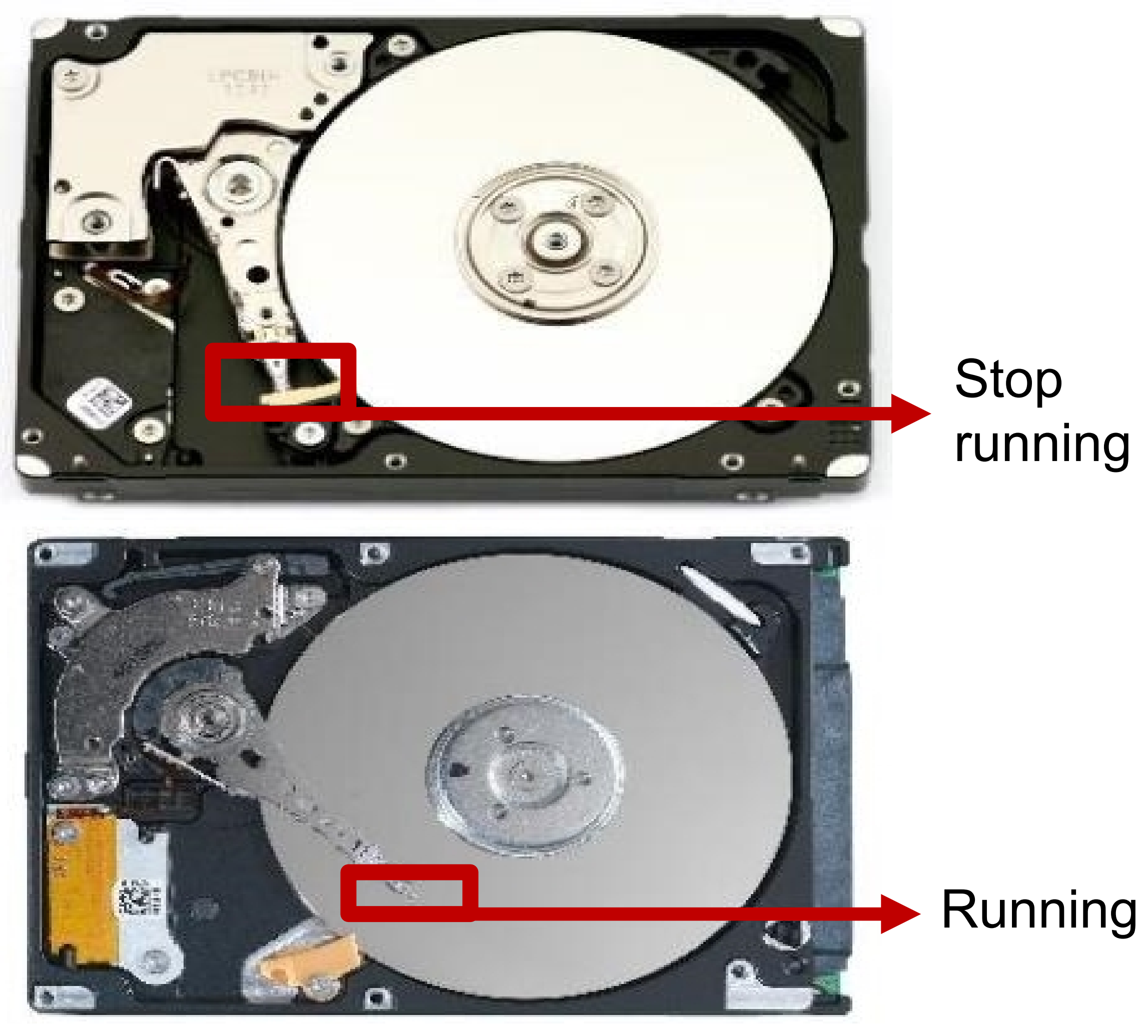
Technology

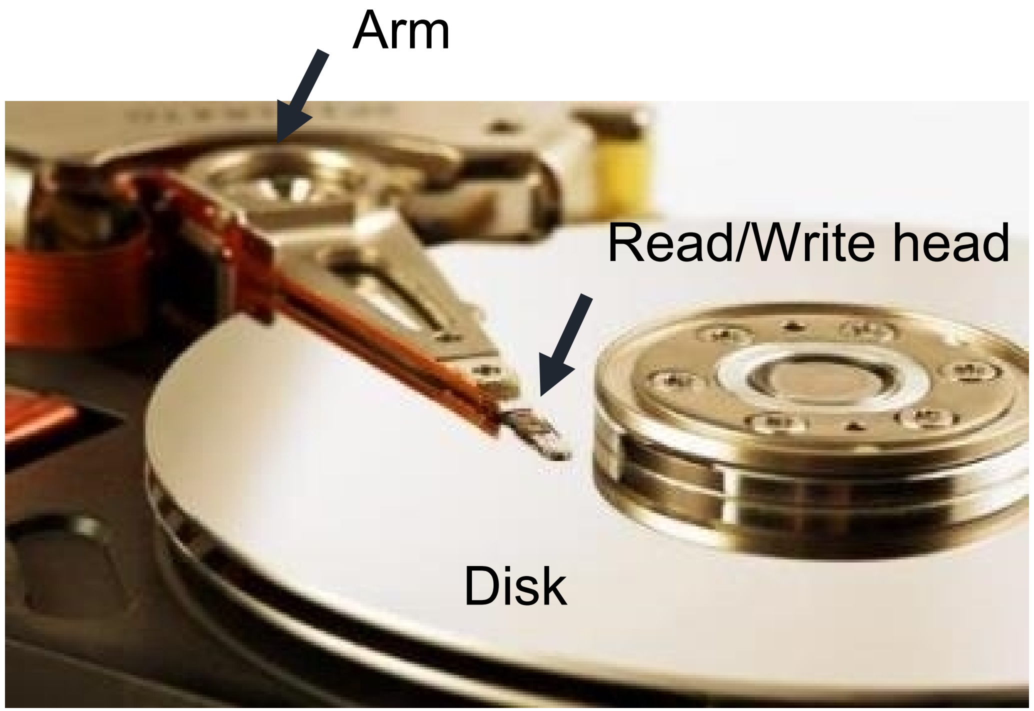
Fire drill knocks ING bank's data centre offline

Why?

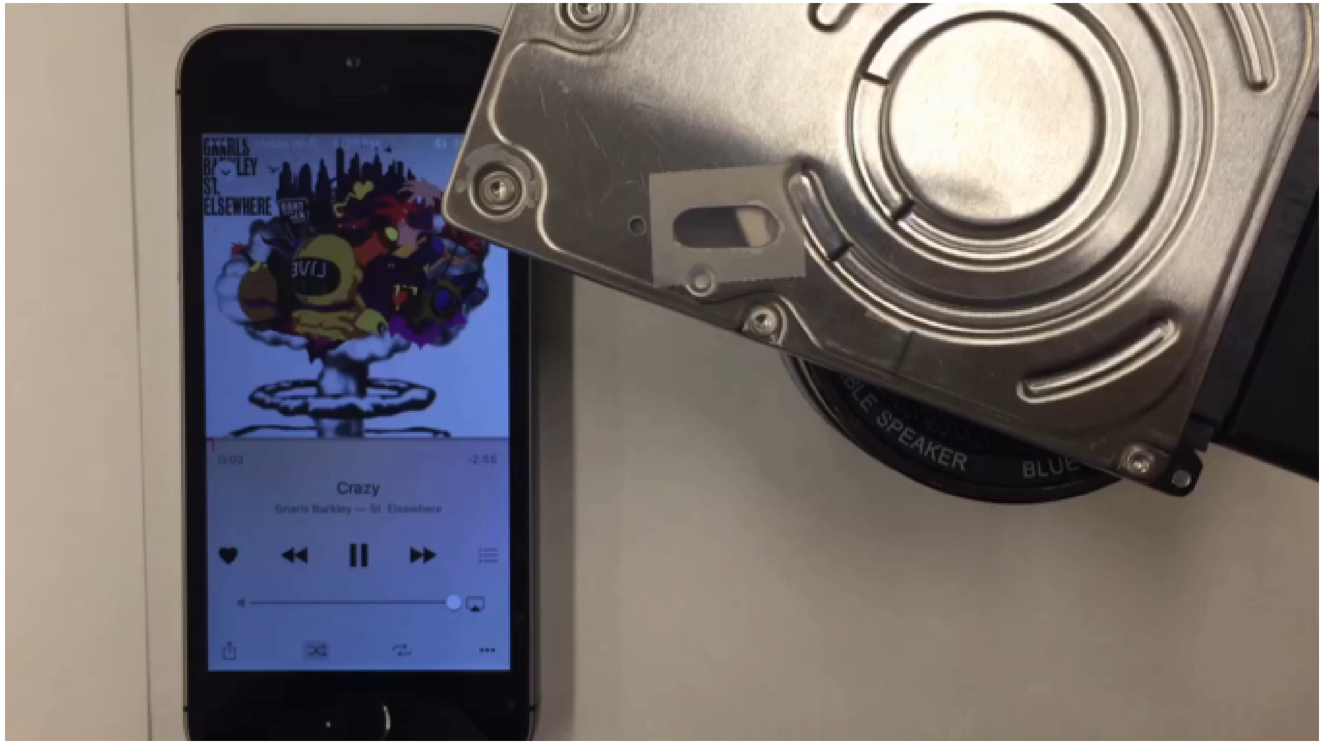
Fire drill knocks ING bank’s data center offline

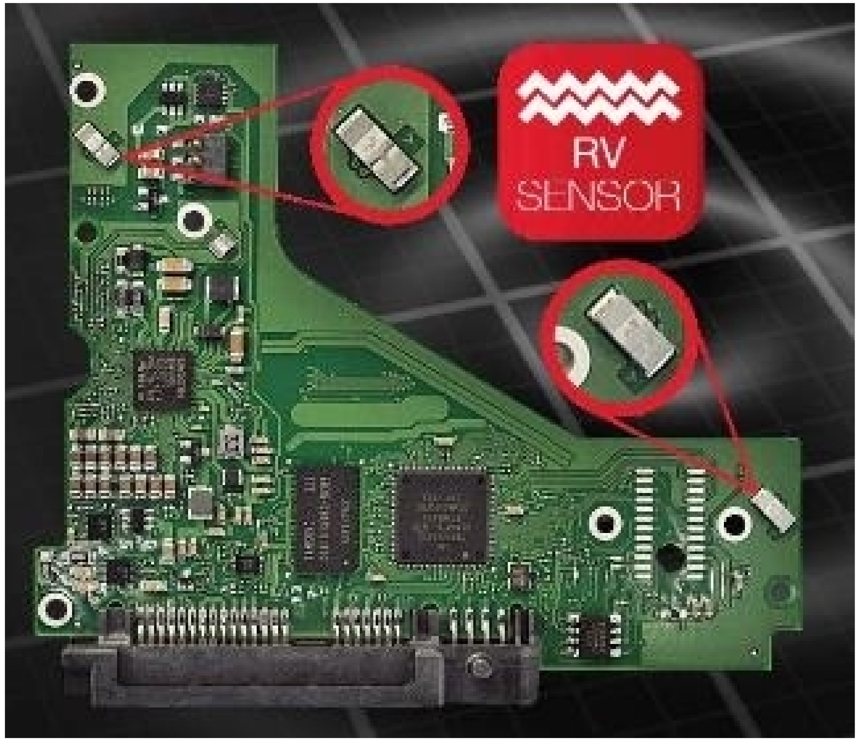
1.1 Out-of-Range: Sound into Vibration Sensors → Drive Failure





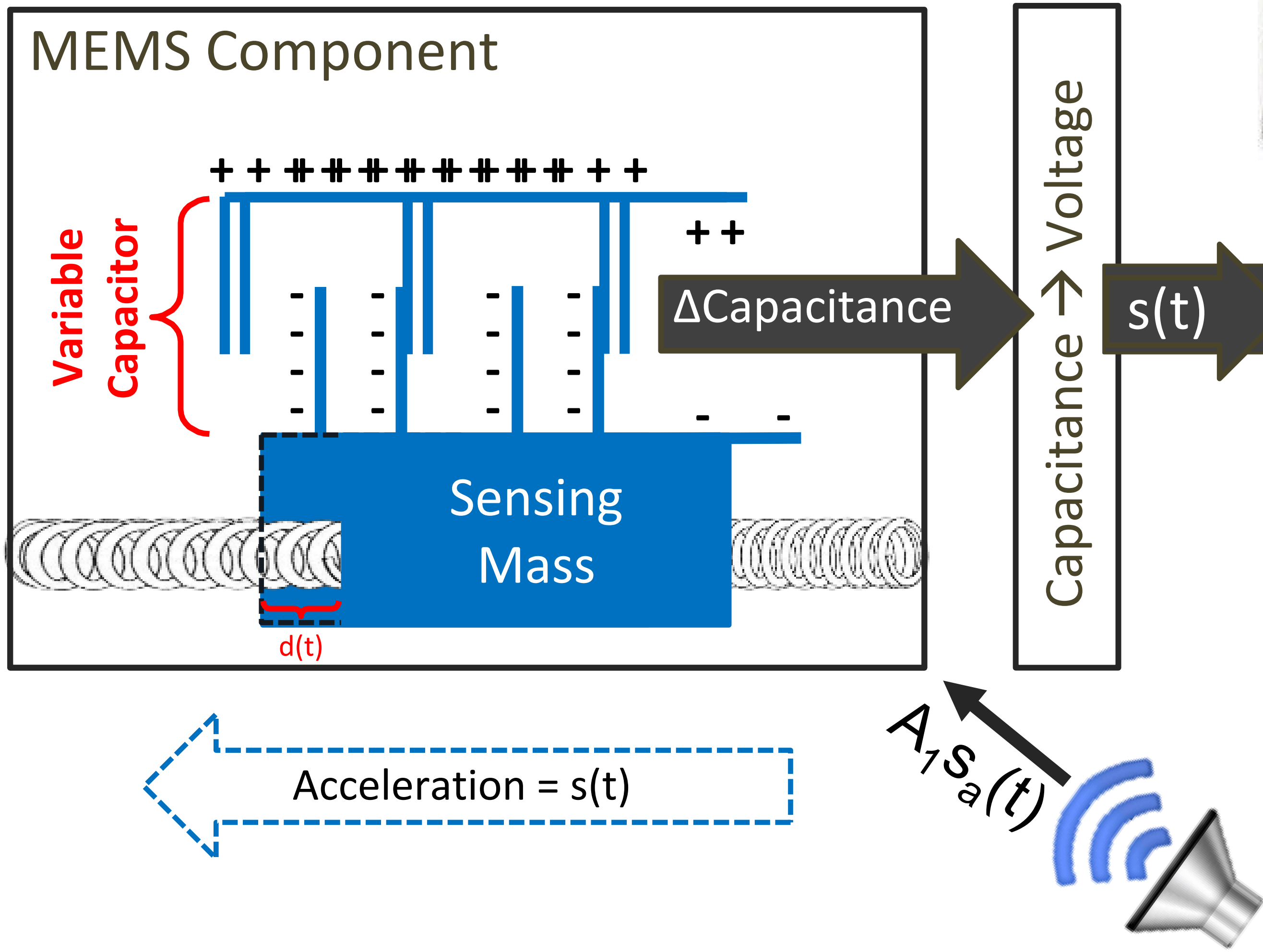
1.1 Out-of-Range: Sound into Vibration Sensors → Drive Failure

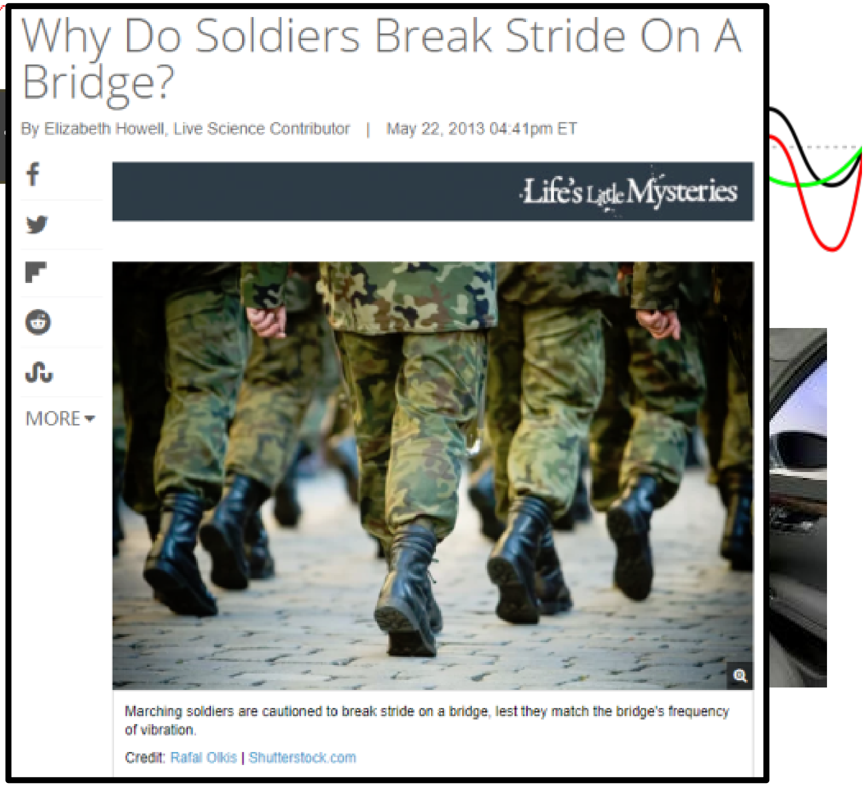




Vibration sensor

1.1 Out-of-Range: Sound into Vibration Sensors → Drive Failure





Why Do Soldiers Break Stride On A Bridge?

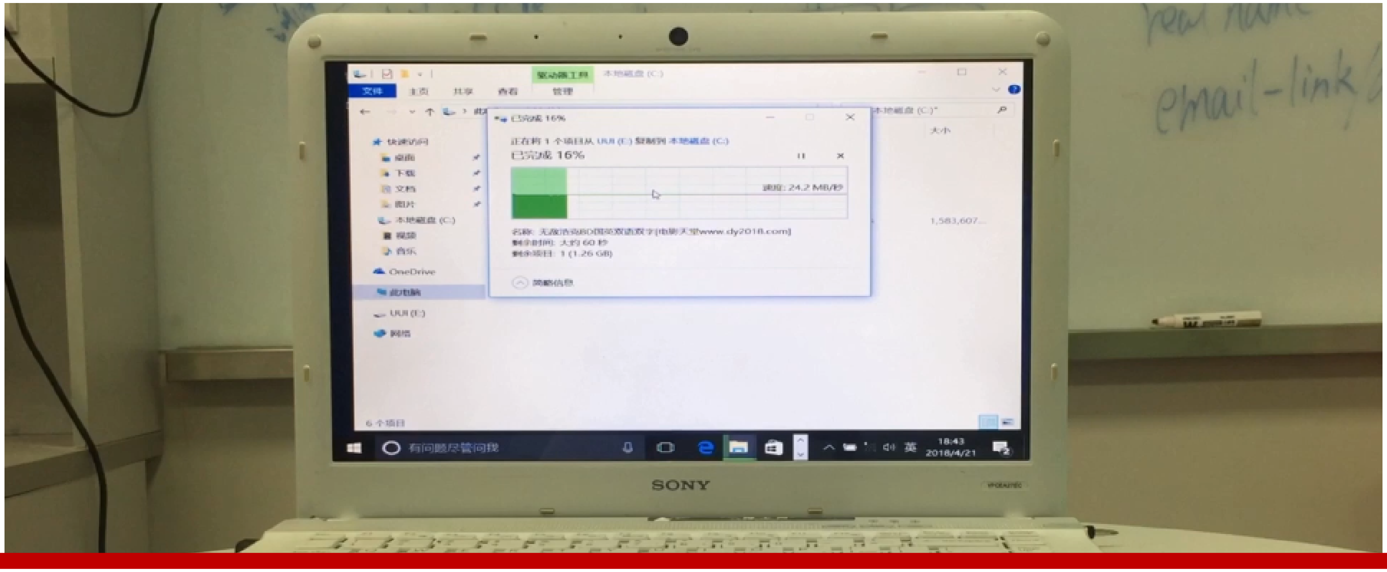
By Elizabeth Howell, Live Science Contributor | May 22, 2013 04:41pm ET

Marching soldiers are cautioned to break stride on a bridge, lest they match the bridge's frequency of vibration.

Credit: Rafal Olkis | Shutterstock.com

1.1 Out-of-Range: Sound into Vibration Sensors → Drive Failure

Normal Signal low-frequency motion signals **VS** **Out-of-Range Signal** high-frequency sound waves

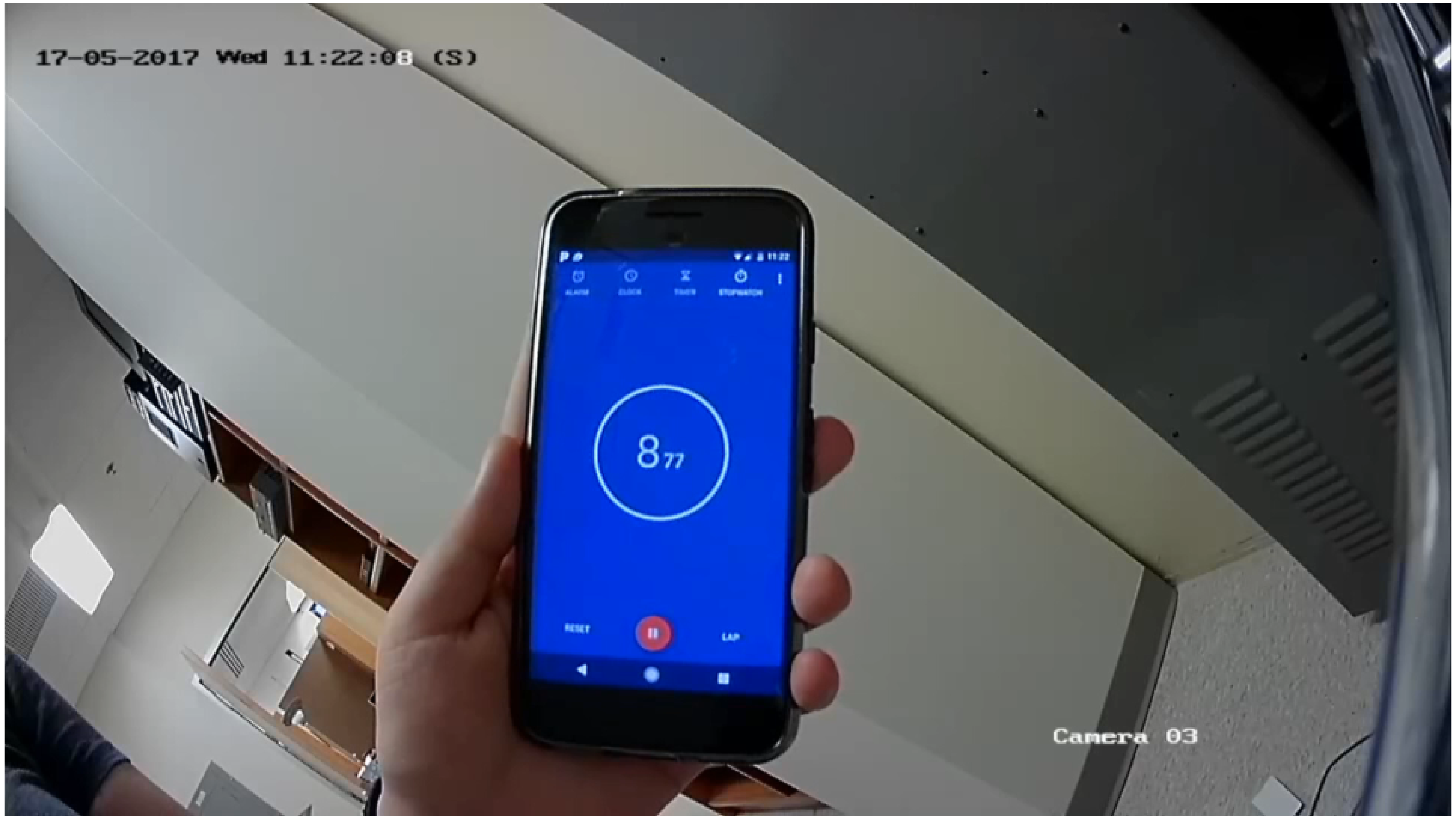


SMART failure predicted on hard disk.

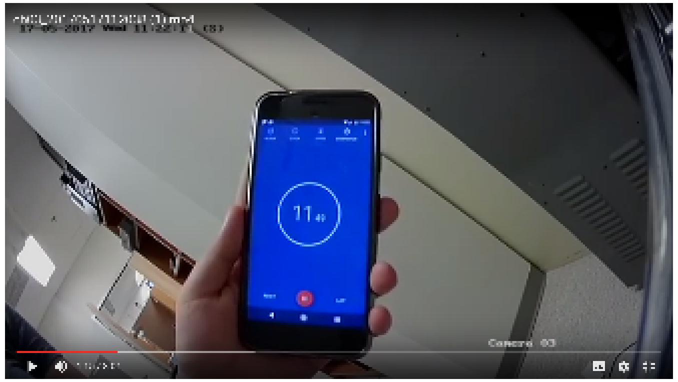
Warning: Immediately back-up your data and replace your hard disk drive

C. Bolton, S. Rampazzi, C. Li, A. Kwong, W. Xu and K. Fu."Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems," S&P 2018

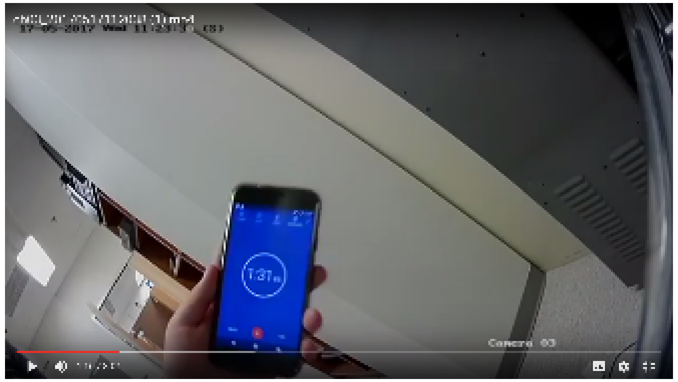
1.2 Out-of-Range: Surveillance System



80s of video missing



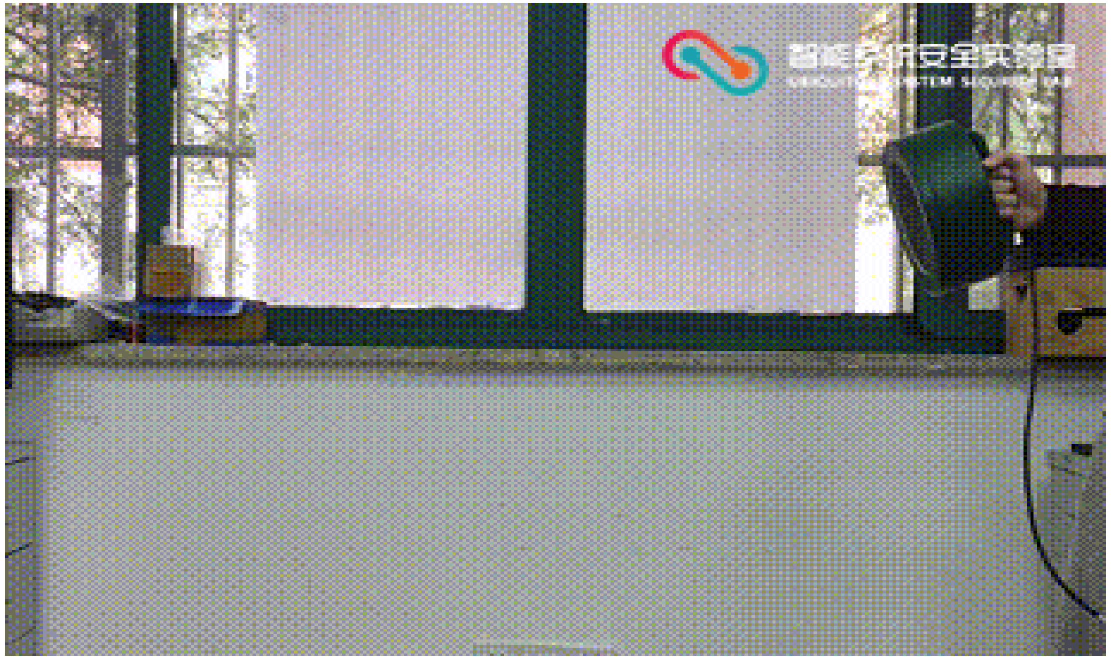
11s

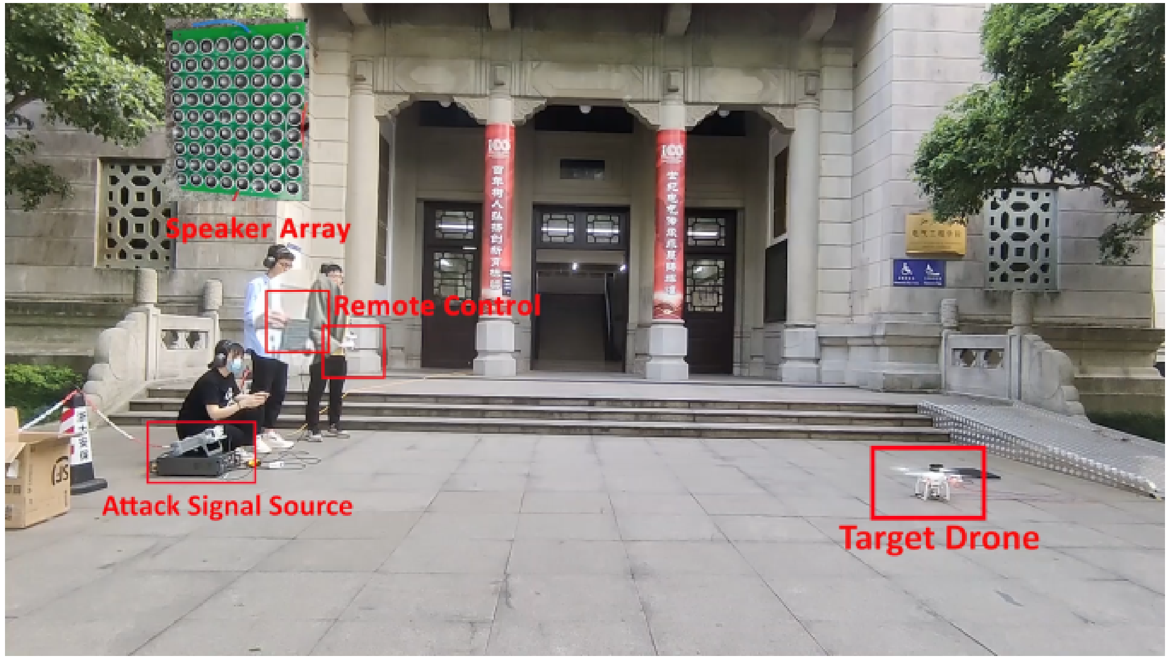


1:31s

1.3 Out-of-Range: Sound Affects IMU→ Drone Drops

Normal Signal low-frequency motion signals VS **Out-of-Range Signal** high-frequency sound waves

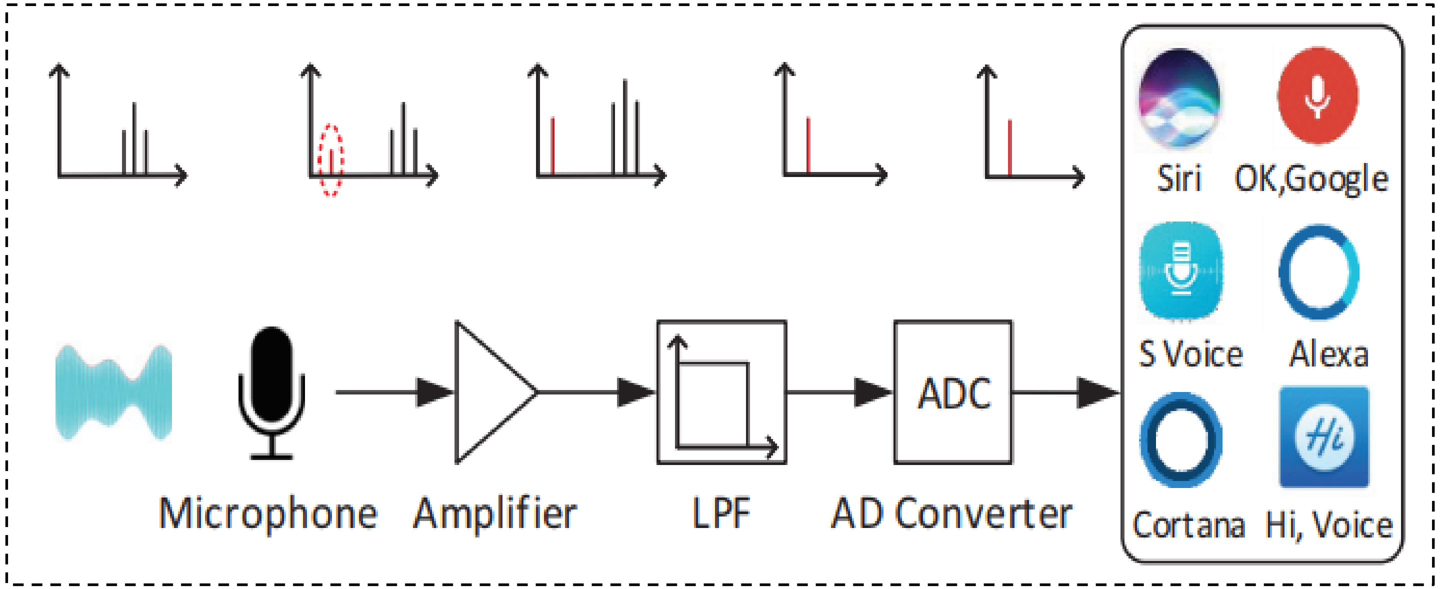




Yunmok Son, Hocheol Shin, Dongkwan Kim, et al. “Rocking drones with intentional sound noise on gyroscopic sensors,” USENIX Security ’15.

1.4 Out-of-Range: MEMS Microphones

Normal Signal voice signal VS **Out-of-Range Signal** ultrasonic signal



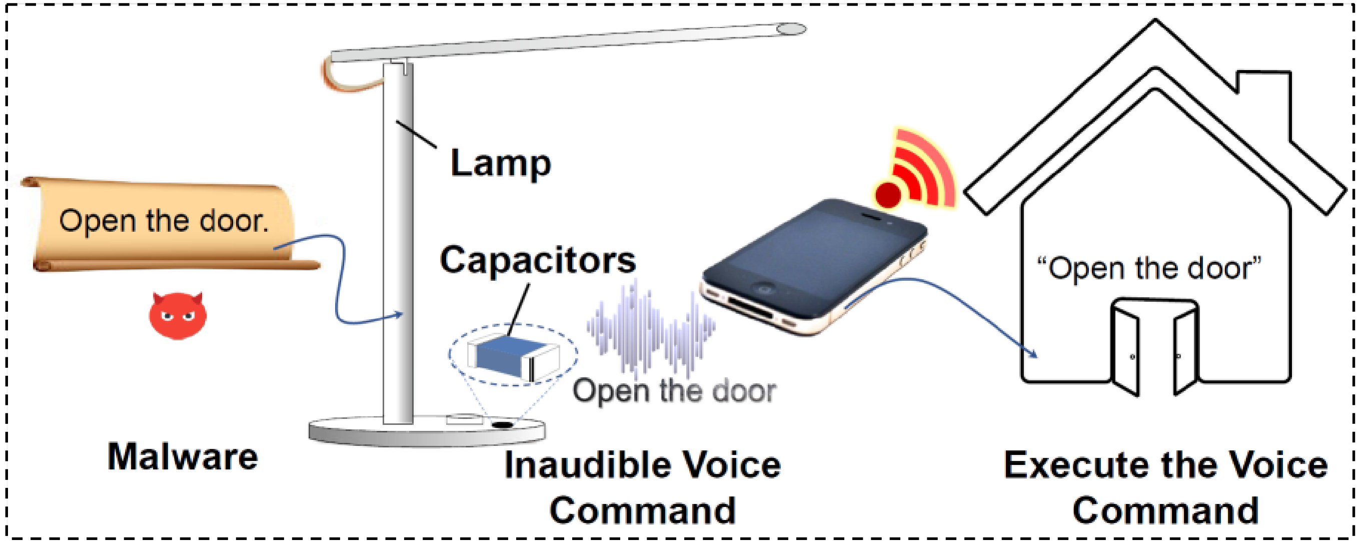
Principle

Demo

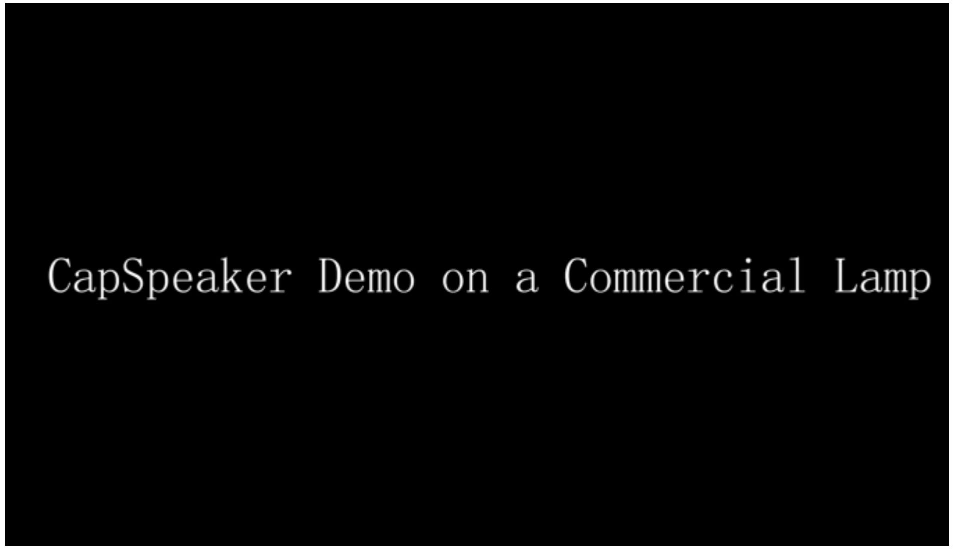
Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. “DolphinAttack: Inaudible Voice Commands,” CCS ’17.

1.5 Out-of-Range: Capacitors

Normal Signal voice signal VS **Out-of-Range Signal** ultrasonic signal



Principle



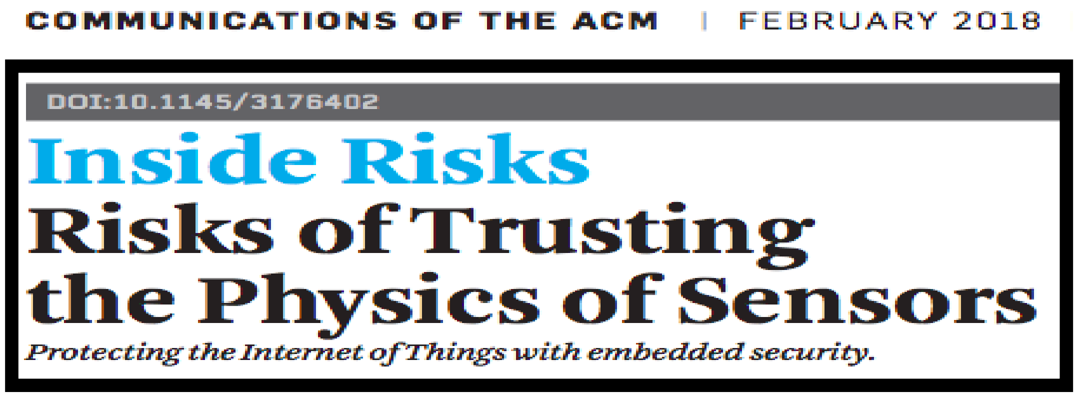
CapSpeaker Demo on a Commercial Lamp

Demo

Xiaoyu Ji, Juchuan Zhang, Shui Jiang, Jishen Li, and Wenyuan Xu. "CapSpeaker: Injecting Voices to Microphones via Capacitors," CCS '21.

2. Cross-Sensing

Root cause: Sensors are supposed to sense only specific physical quantities, but can sense other spurious physical quantities and lead to anomalous results and operations



COMMUNICATIONS OF THE ACM | FEBRUARY 2018

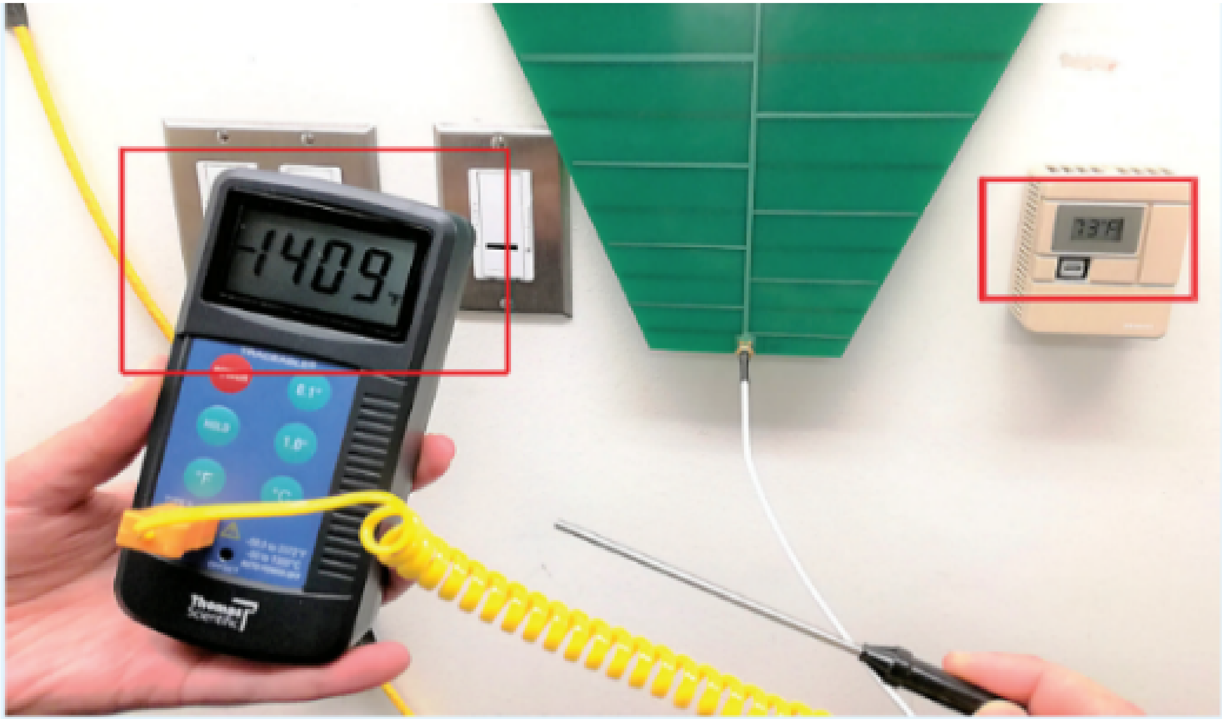
DOI:10.1145/3176402

Inside Risks

Risks of Trusting the Physics of Sensors

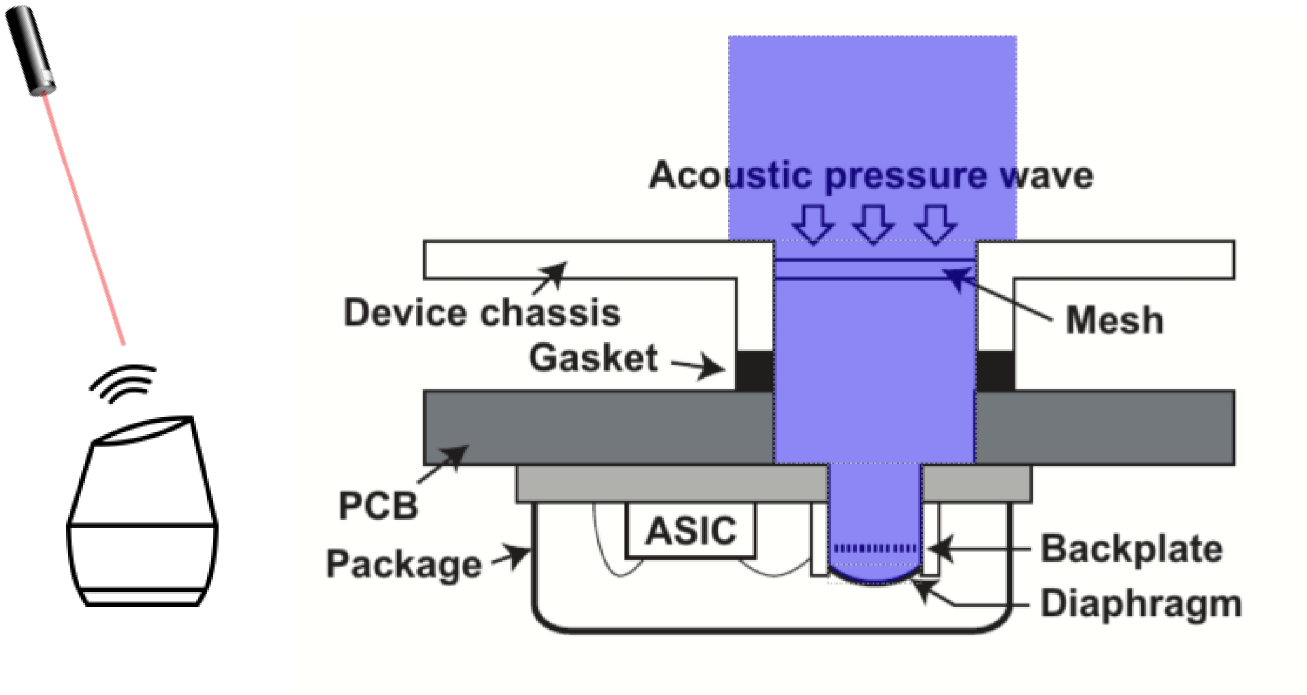
Protecting the Internet of Things with embedded security.

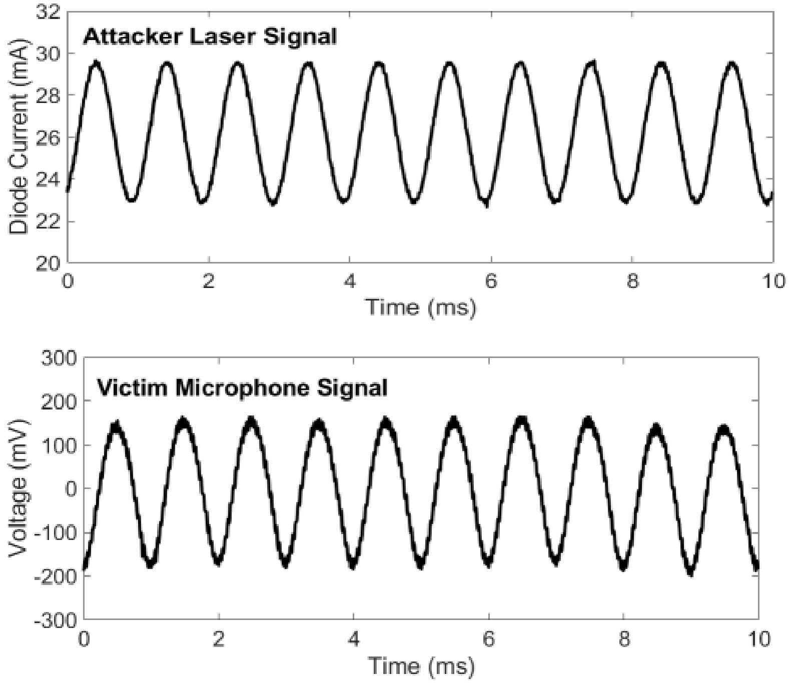
- **Physical signals directly affect thermocouple thermometers**
  - Thermocouples measure voltage to infer temperature
  - It is not always the temperature that induces the voltage



2.1 Cross-Sensing: Light → Voice Commands

Reality: Microphones capture **acoustic** signals & LIGHT signals



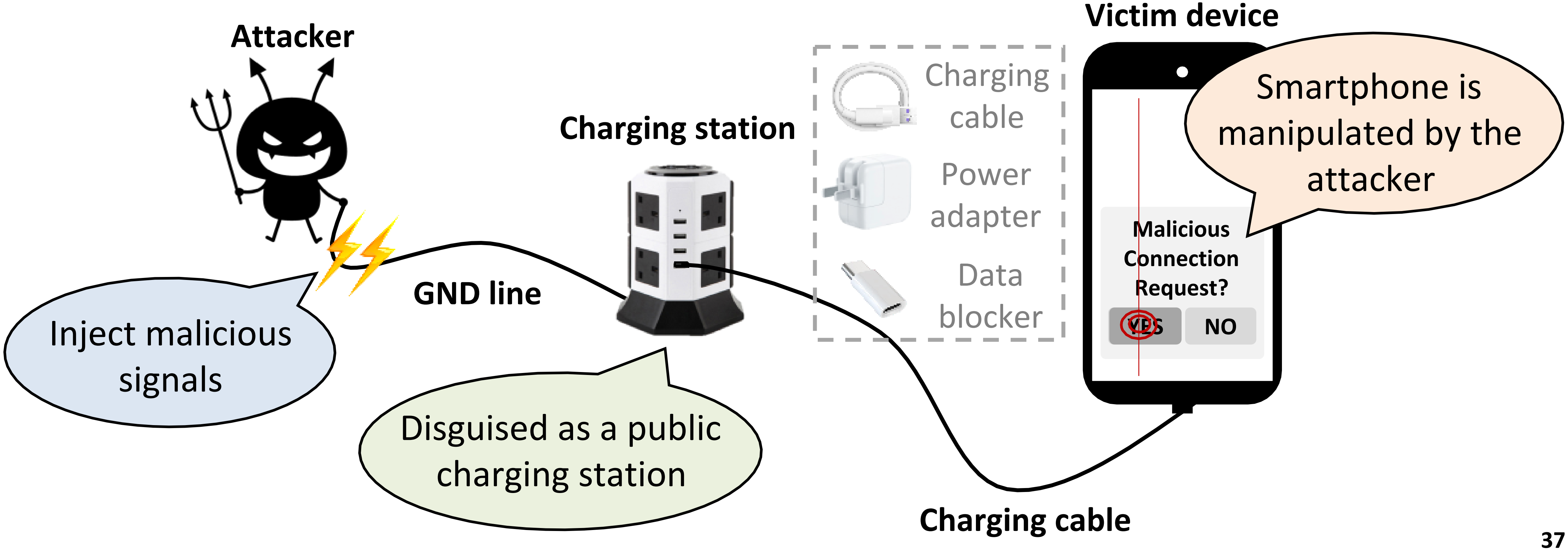


2.1 Cross-Sensing: Light → Voice Commands

Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu. Light commands: laser-based audio injection attacks on voice-controllable systems. USENIX Security '20.

2.2 Cross-Sensing: Charging Cable Signals→ Contact Sensing

Normal Sensing sensing finger touch VS **Cross-Sensing** sensing malicious electronic signals



Attacker

Inject malicious signals

GND line

Charging station

Disguised as a public charging station

Charging cable

Power adapter

Data blocker

Victim device

Smartphone is manipulated by the attacker

Malicious Connection Request?

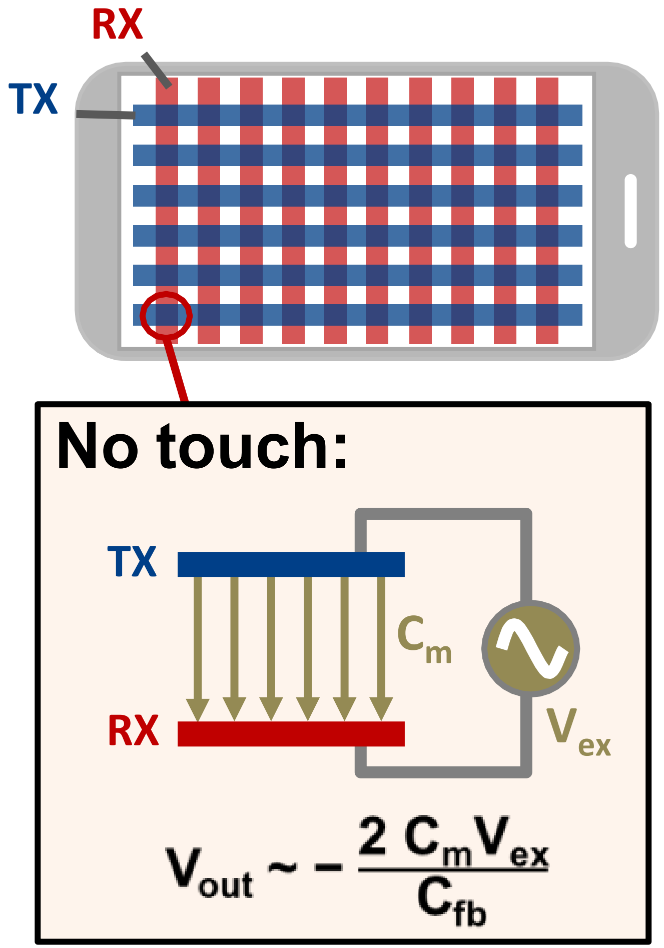
YES **NO**

Charging cable

Yan Jiang, Xiaoyu Ji, Chen Yan, Richard Mitev, Ahmad-Reza Sadeghi, and Wenyuan Xu. " WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens," S&P 2022.

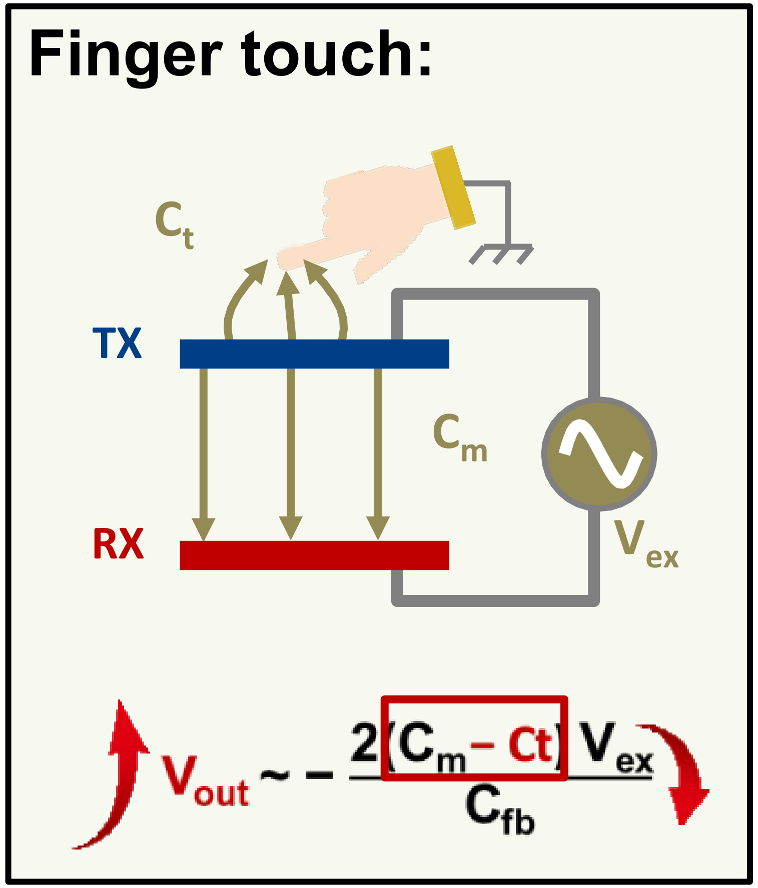
2.2 Cross-Sensing: Charging Cable Signals→ Contact Sensing

How capacitive touchscreens work?



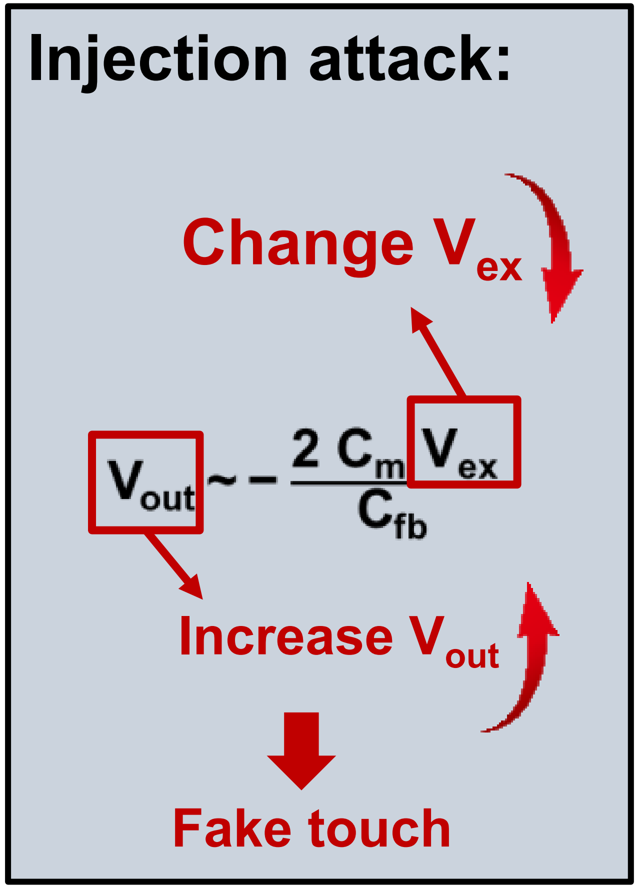
No touch:

$$V_{out} \sim -\frac{2\,C_m V_{ex}}{C_{fb}}$$



Finger touch:

$$V_{out} \sim -\frac{2\boxed{(C_m - Ct)}\,V_{ex}}{C_{fb}}$$



Injection attack:

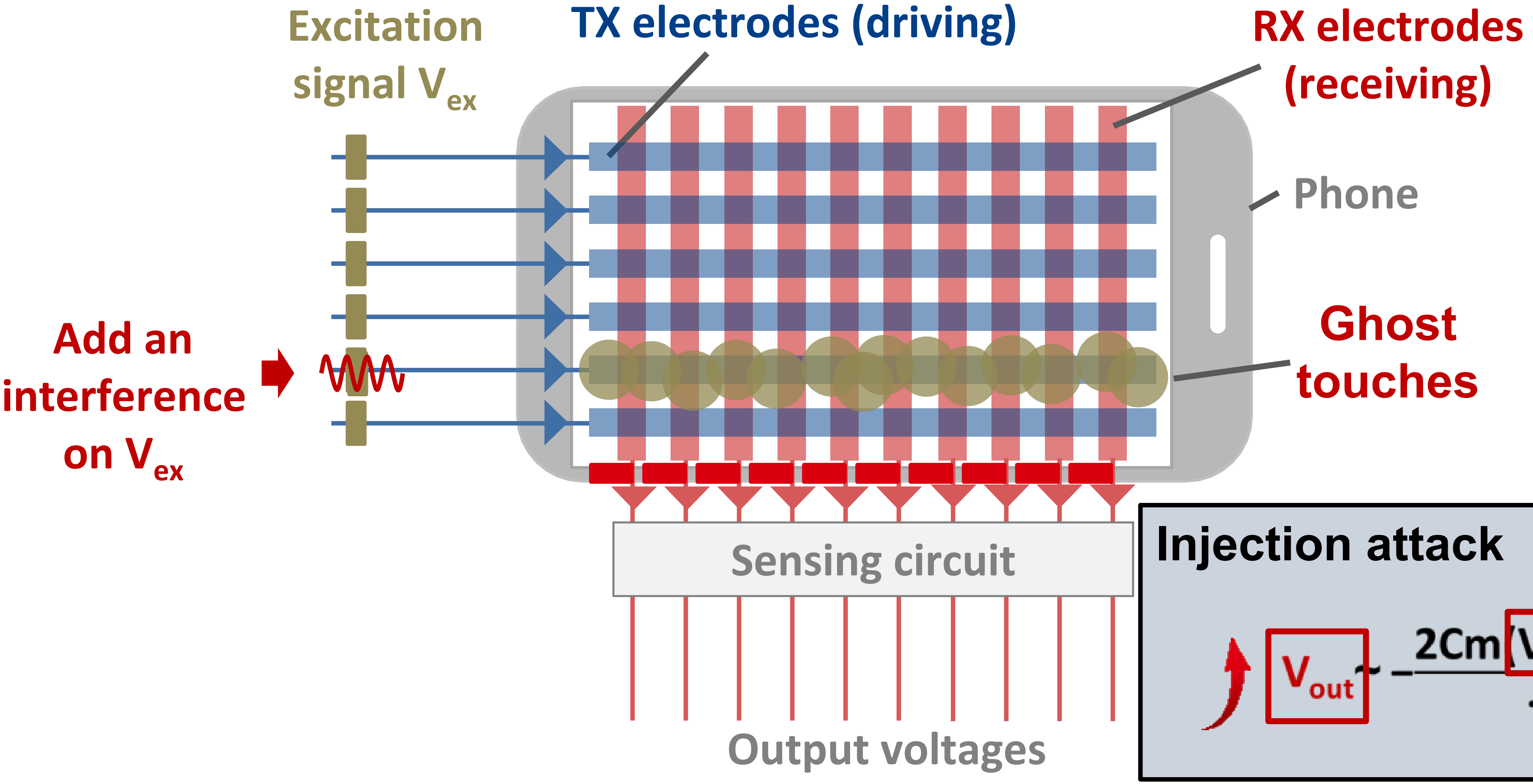
Change V_{ex}

$$\boxed{V_{out}} \sim -\frac{2\,C_m \boxed{V_{ex}}}{C_{fb}}$$

Increase V_{out}

Fake touch

2.2 Cross-Sensing: Charging Cable Signals→ Contact Sensing


Excitation signal V_{ex}
TX electrodes (driving)
RX electrodes (receiving)
Phone
Add an interference on V_{ex}
Ghost touches
Sensing circuit
Output voltages

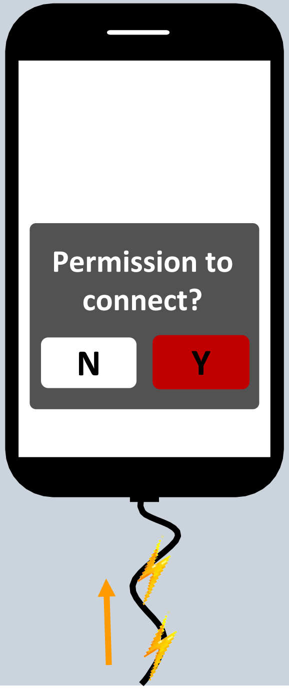
Injection attack

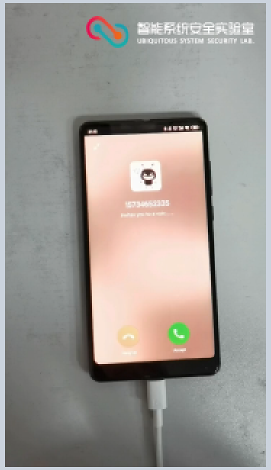
$$\uparrow \boxed{V_{out}} \approx -\frac{2Cm\boxed{(V_{ex}-V_{att})}}{C_{fb}} \downarrow$$

2.2 Cross-Sensing: Charging Cable Signals→ Contact Sensing

- **Injection attack**

  Create ghost touches

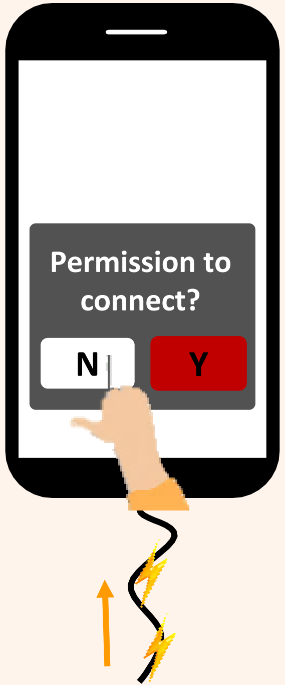




Pick up a phone call

- **Alteration attack**

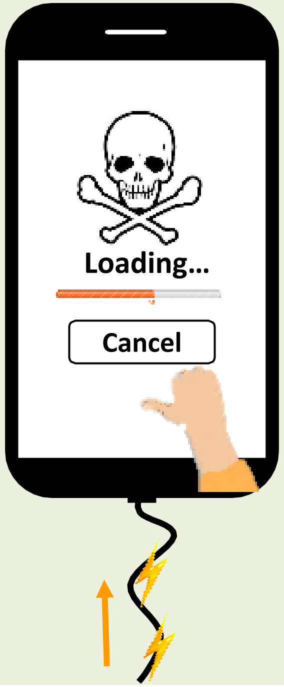
  Change the user input



"Decline"
→ "Accept"

- **DoS attack**

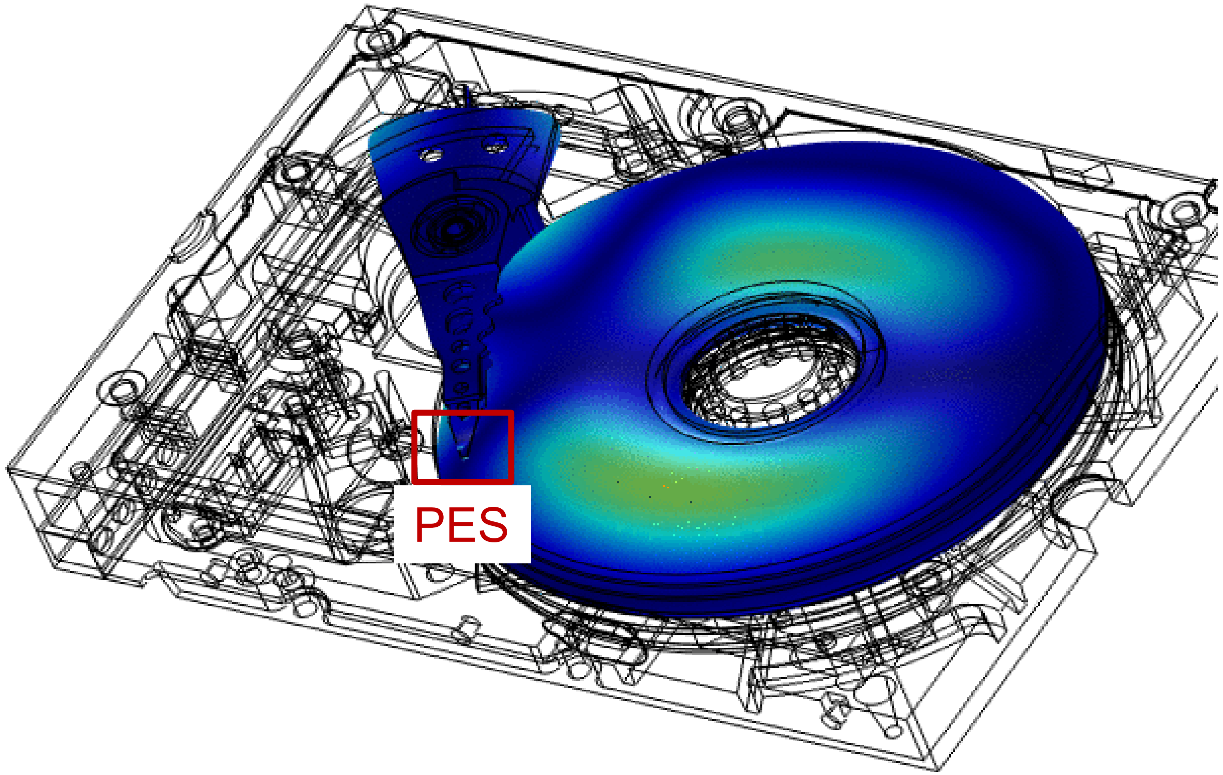
  Disable the touch input

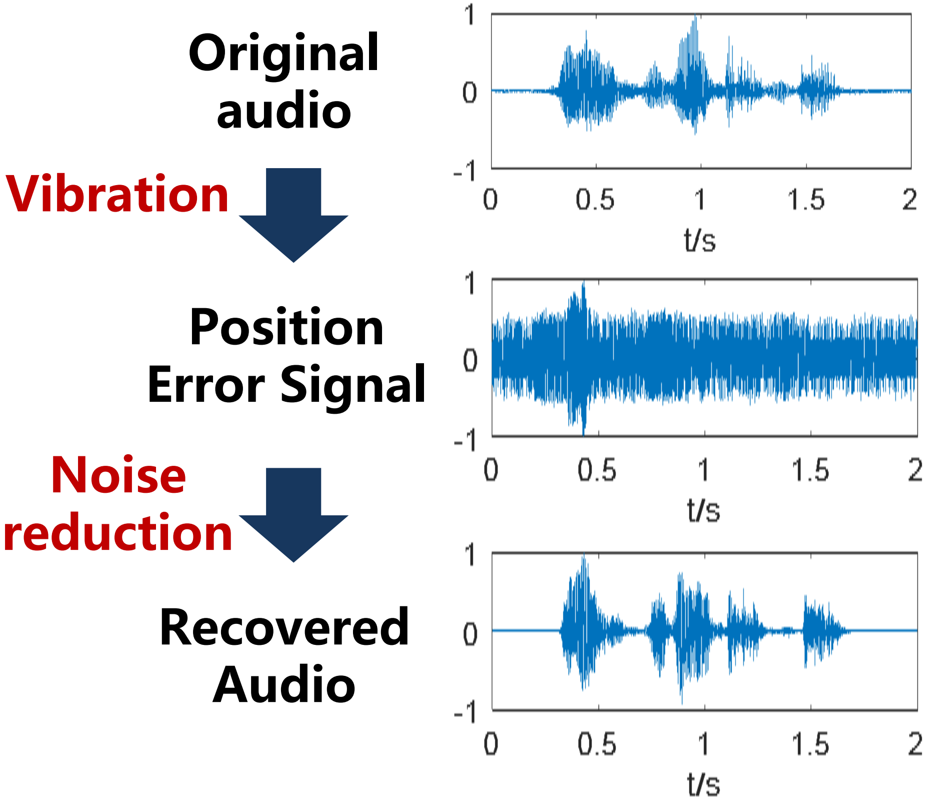


Can not operate the phone

2.3 Cross-Sensing: Sound Wave → Position Error Signal

Normal sensing Position Error Signal VS **Cross-sensing** Sound wave signal




Original audio

Vibration

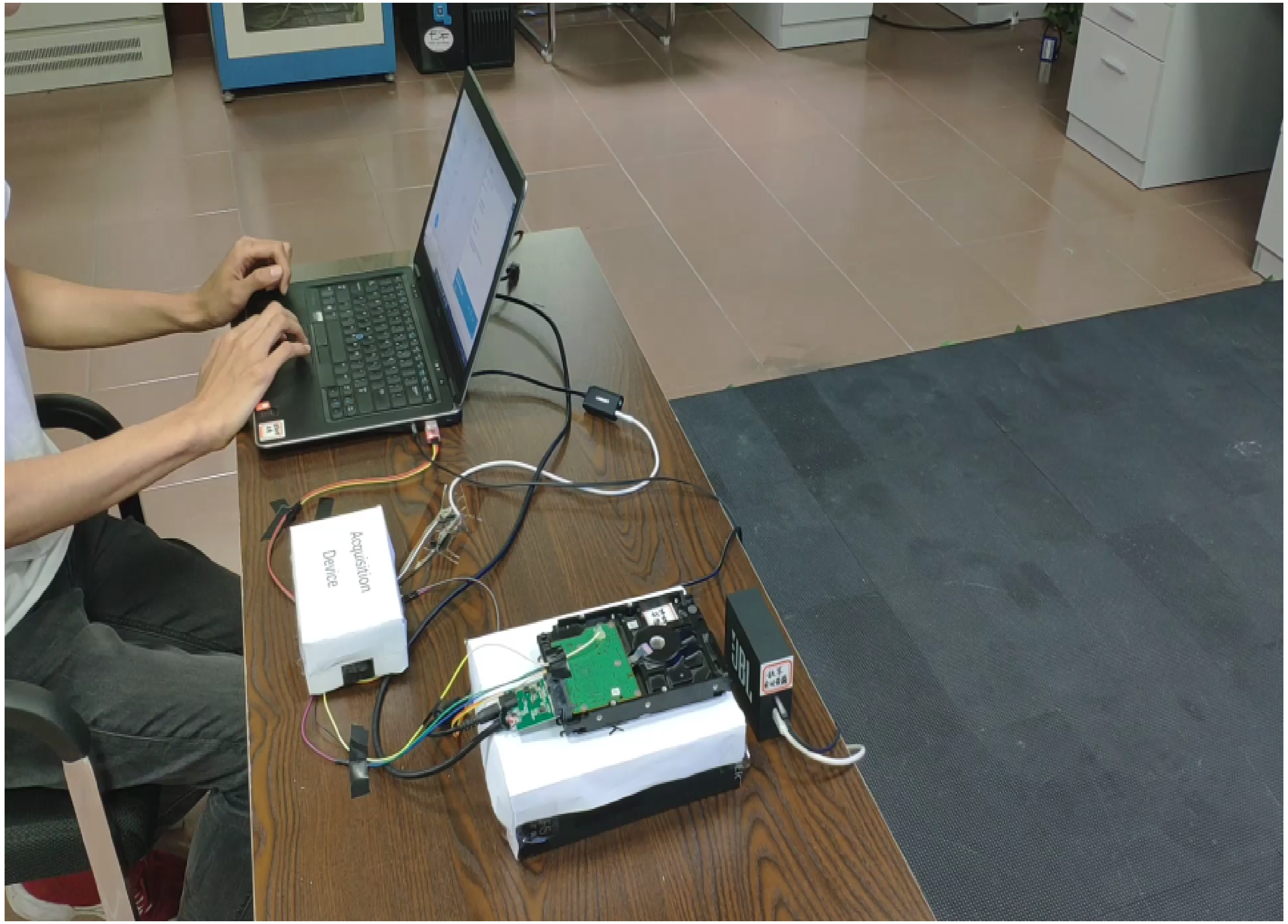
Position Error Signal

Noise reduction

Recovered Audio

Andrew Kwong, Wenyuan Xu, and Kevin Fu. "Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone," S&P 2019

2.3 Cross-Sensing: Sound Wave → Position Error Signal



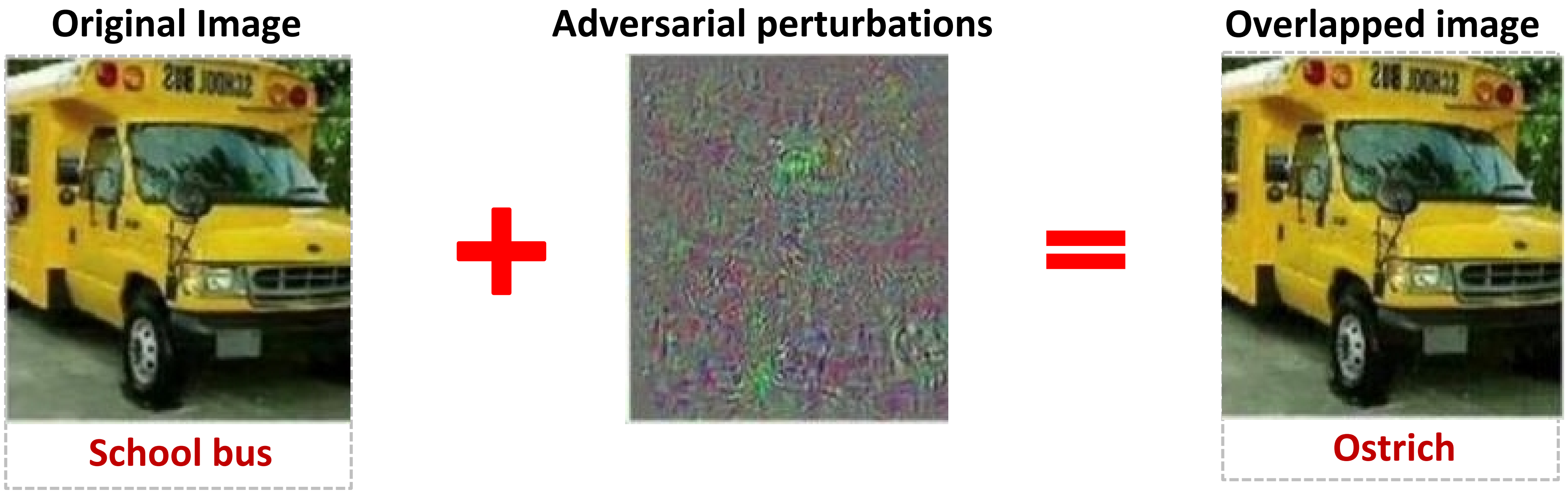
original

raw

filtered

3. Adversary Input

Root cause: An input in the physical domain causes an adversarial example in the cyber domain, resulting in misclassification or misdetection



Original Image

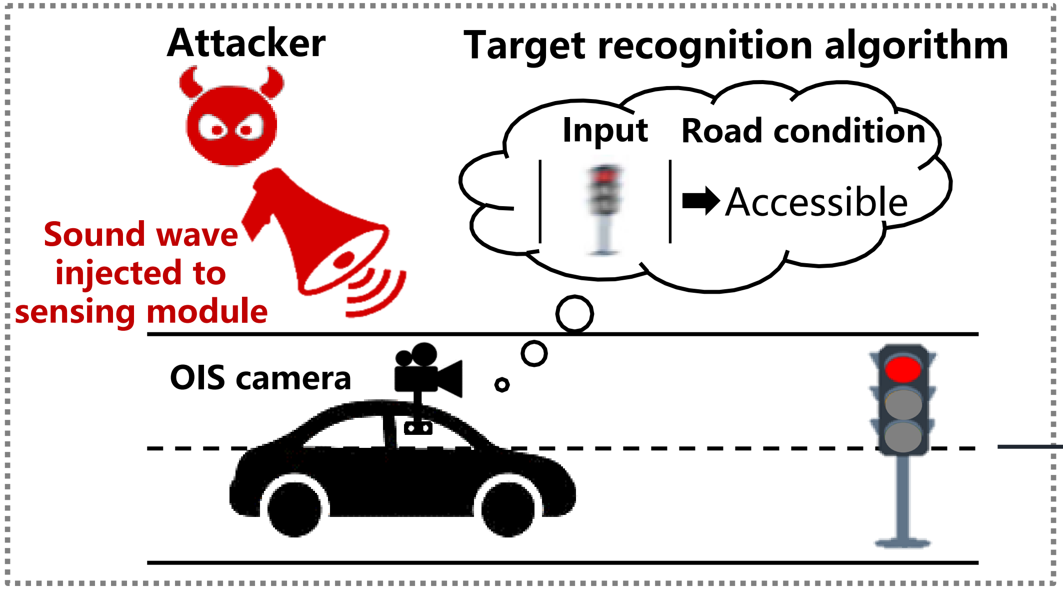
Adversarial perturbations

Overlapped image

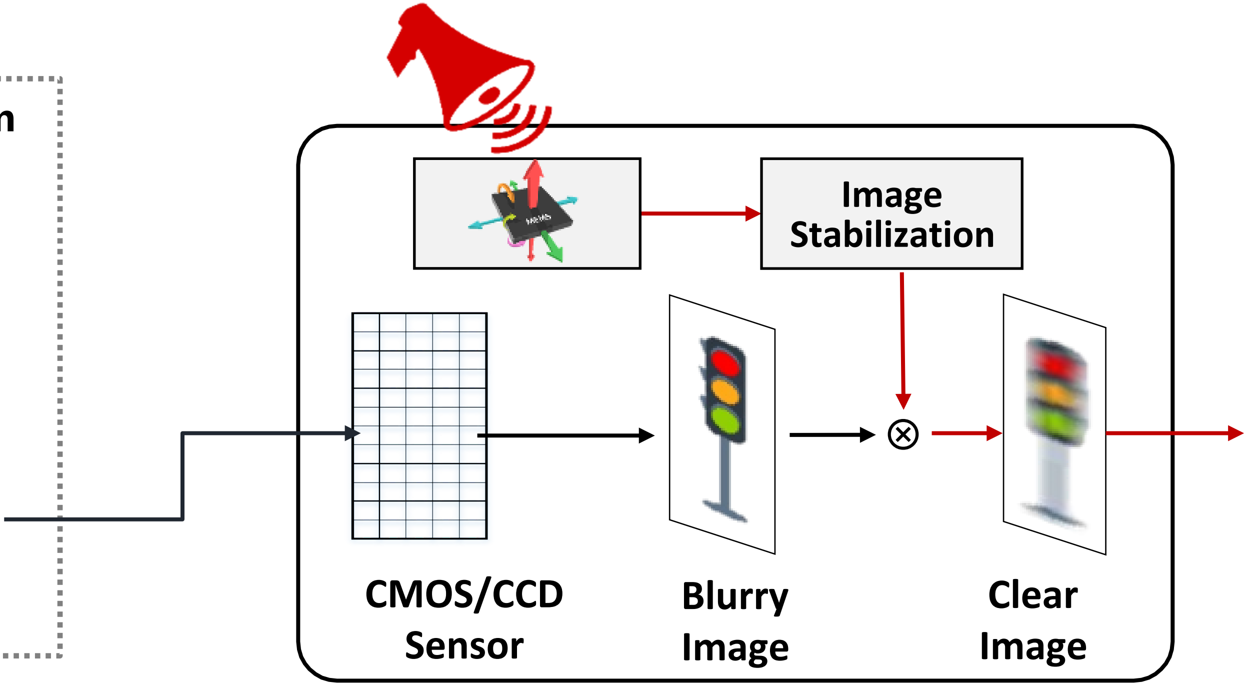
Image adversarial example attack

3.1 Adversary Input: Blurred Image→ Recognition Error

Normal vehicle → recognize as vehicle VS **Abnormal** blurred vehicle → recognize as pedestrian

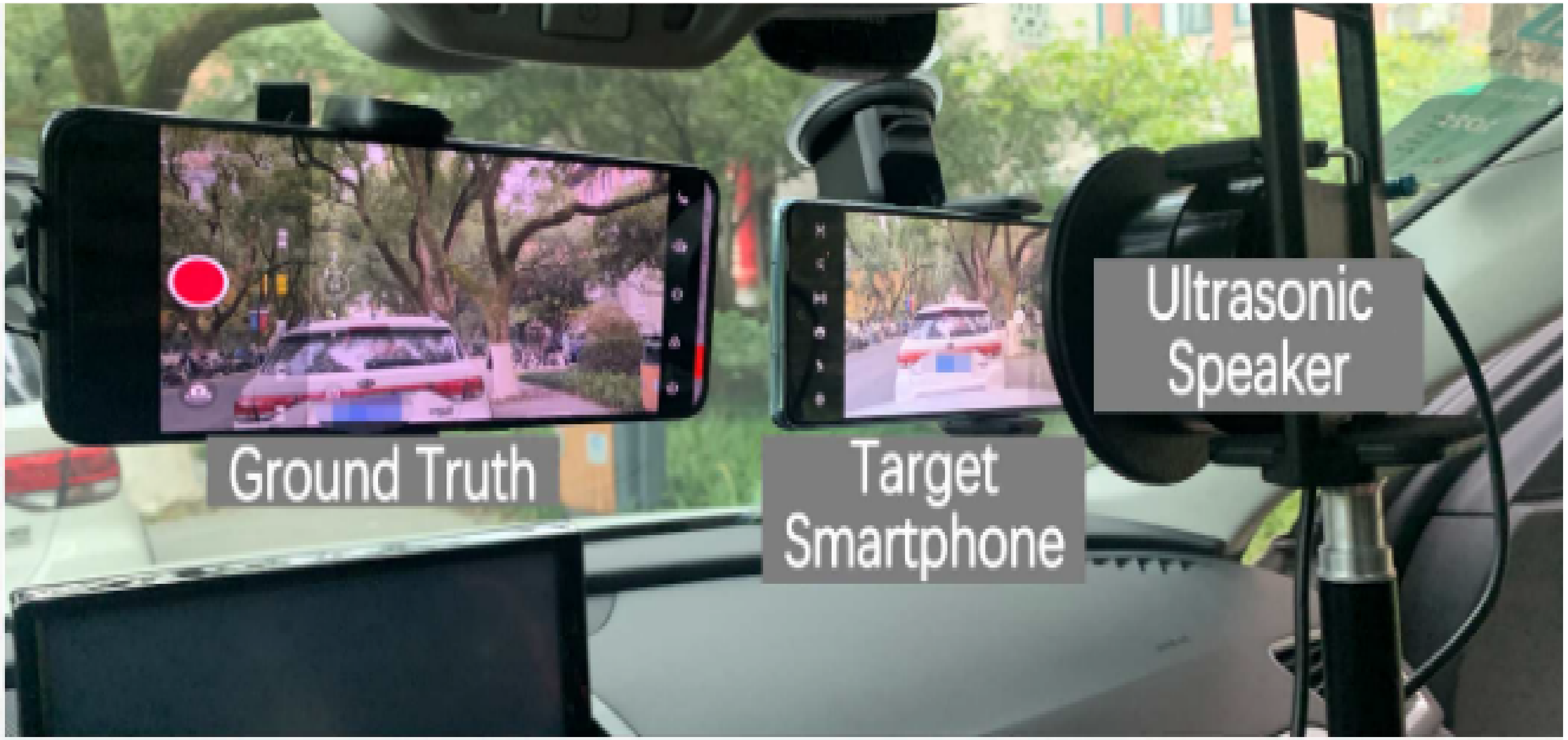

Attacker
Target recognition algorithm
Input
Road condition
➡Accessible
Sound wave injected to sensing module
OIS camera

Attack target: optical image stabilizer (OIS)

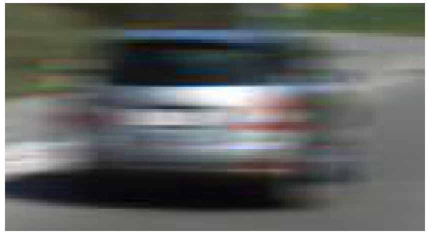


Blurred image generation

3.1 Adversary Input: Blurred Image→ Recognition Error

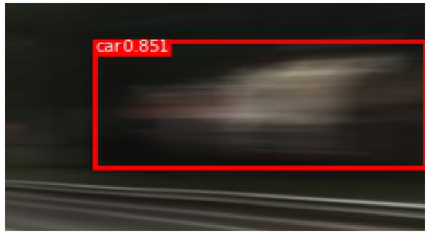


Setup



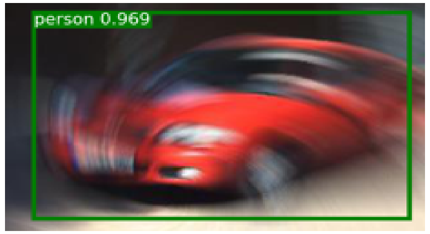
heavy, horizontal

Hiding
“A” → None



heavy, horizontal

Creating
None → “A”



heavy, anticlockwise

Altering
“A” → “B”

Consequences

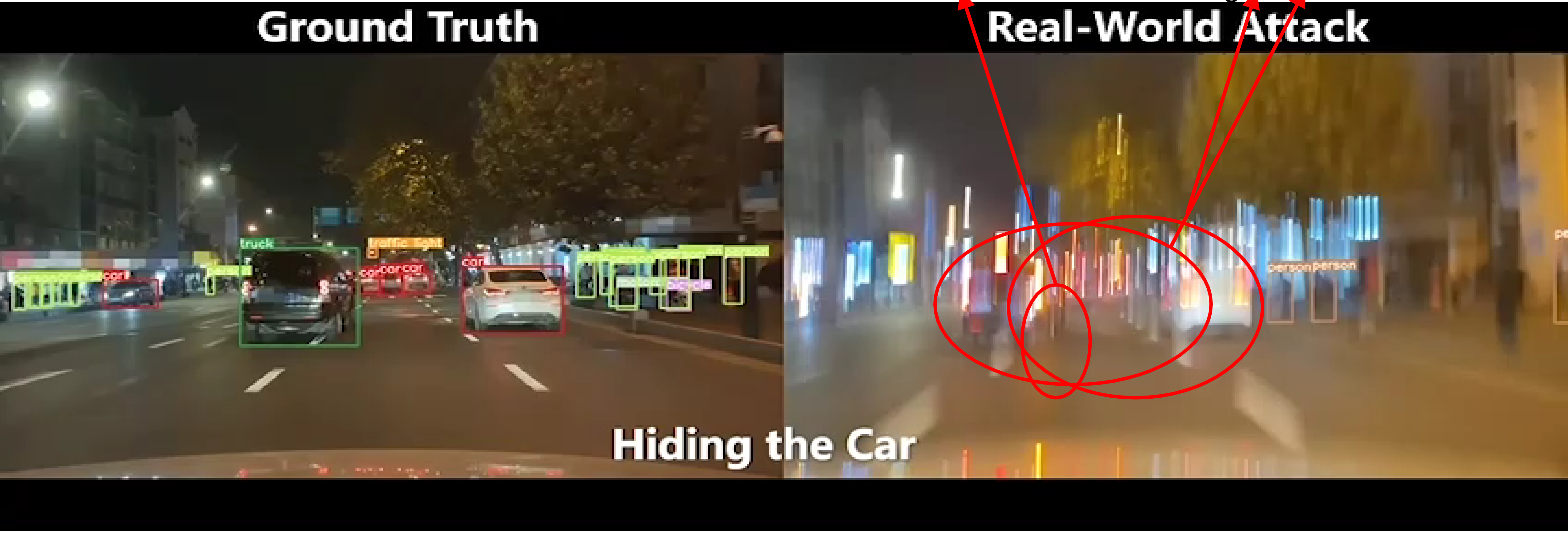
X. Ji and Y. Cheng and Y. Zhang and K. Wang and C. Yan and W. Xu and K. Fu. “Poltergeist: Acoustic Adversarial Machine Learning against Cameras and Computer Vision,”S&P 2021

3.1 Adversary Input: Blurred Image → Recognition Error

The car is recognized as a pedestrian

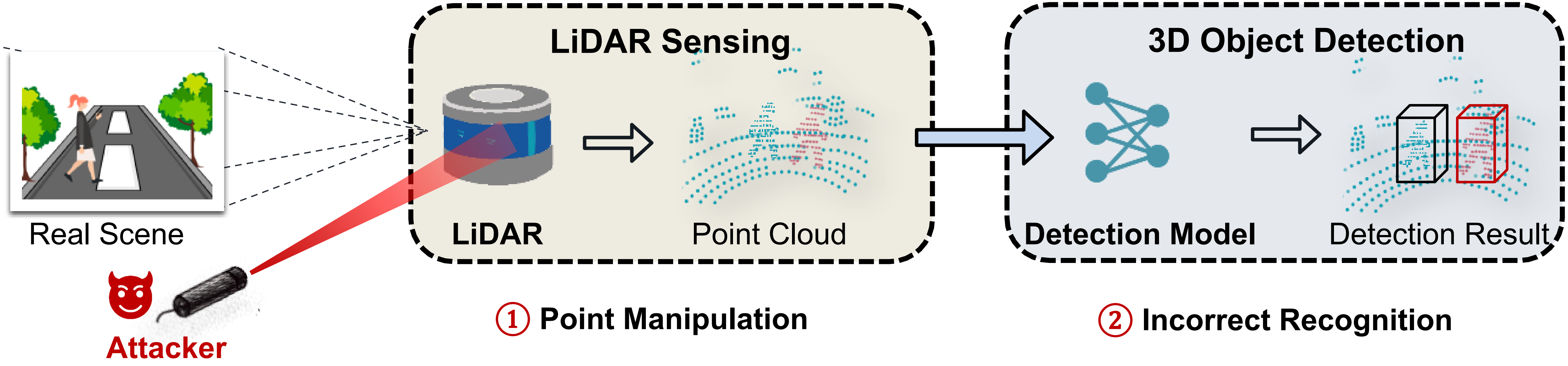
The light is recognized as a truck

The car cannot be recognized



https://github.com/USSLab/PoltergeistAttack

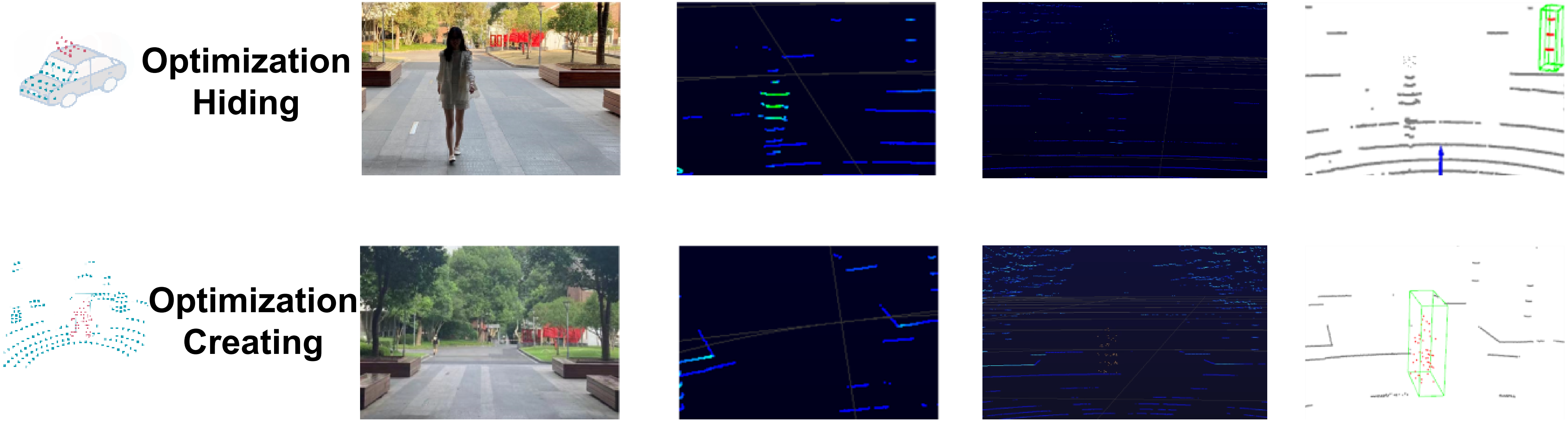
3.2 Adversary Input: Laser → Recognition Error



Attack scenario and principle

Zizhi Jin, Xiaoyu Ji, Yushi Cheng, Bo Yang, Chen Yan and Wenyuan Xu. "PLA-LiDAR: Physical Laser Attacks against LiDAR-based 3D Object Detection in Autonomous." S&P 2023

3.2 Adversary Input: Laser → Recognition Error



Optimization Hiding

Optimization Creating

Point Cloud

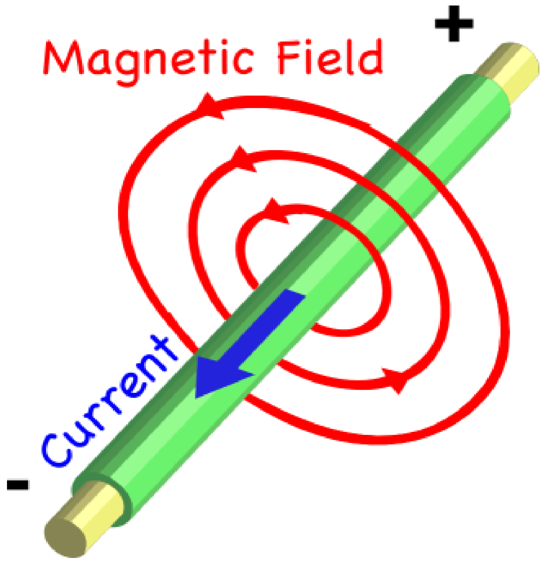
Point Cloud

Attack Detection

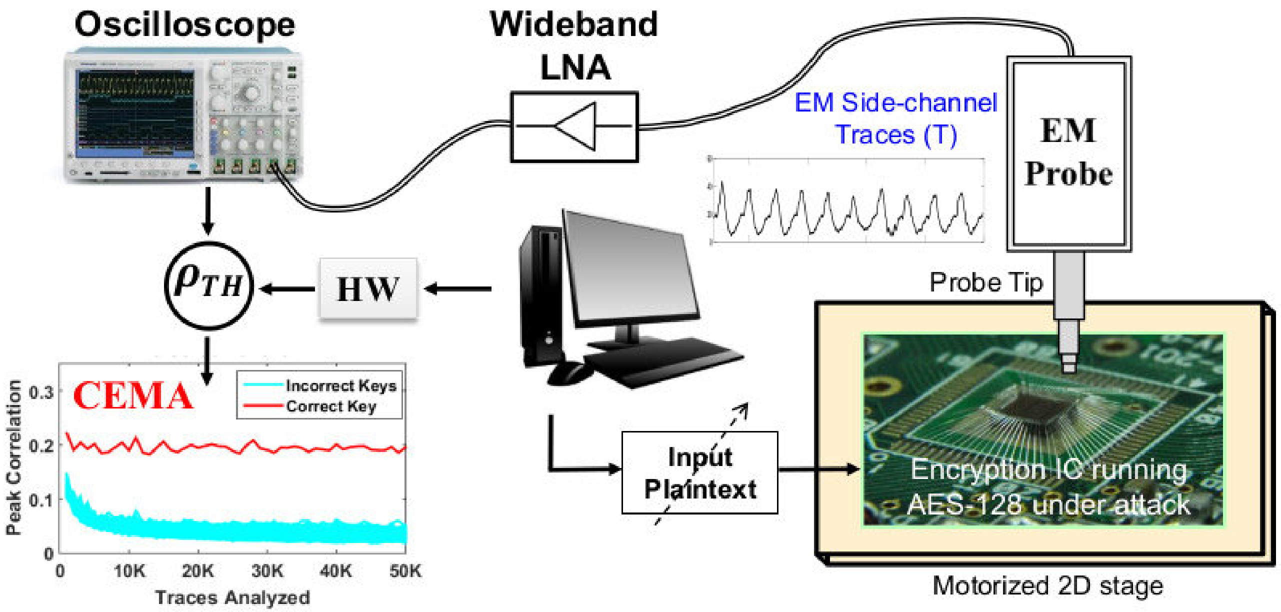
Attack results

4. Side Channel

Root cause: electronic devices such as chips generate multi-physical side channel leakage of electromagnetic, RF, acoustic and optical waves related to the processed information



Biot-Savart Law



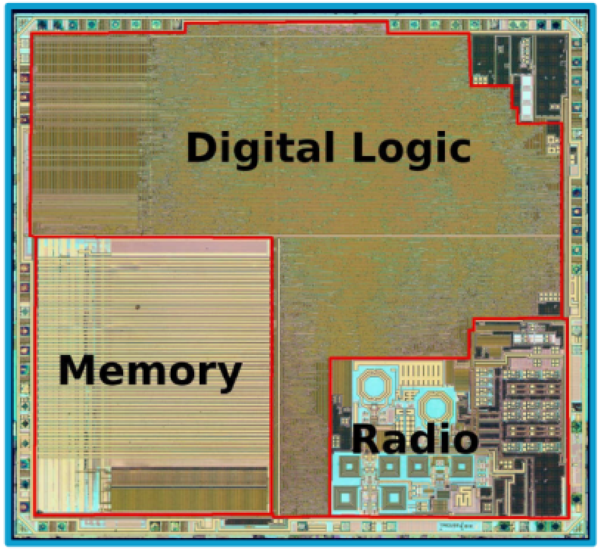
Measuring the EM leak to recover the key

4.1 Side Channel: Encryption algorithm → Bluetooth RF Signal

Side channel encryption algorithm → BT RF signal

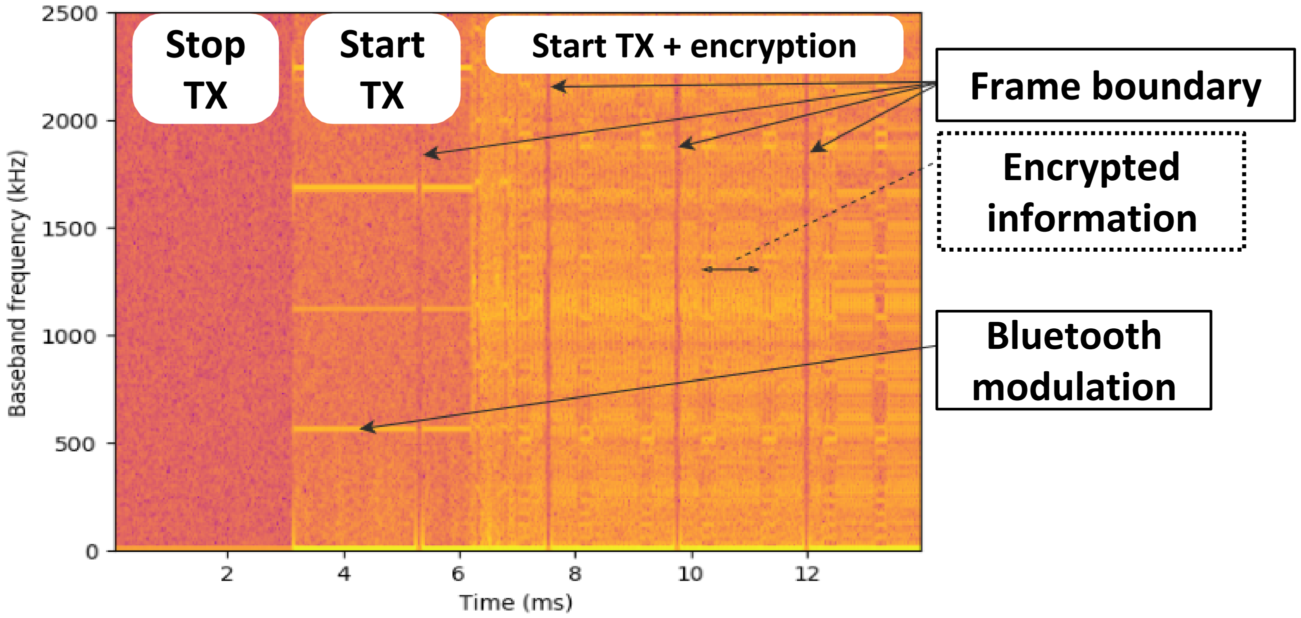
Mixed-signal chip

Encryption algorithm AES-128



Bluetooth RF signal

Encryption information coupled via substrate

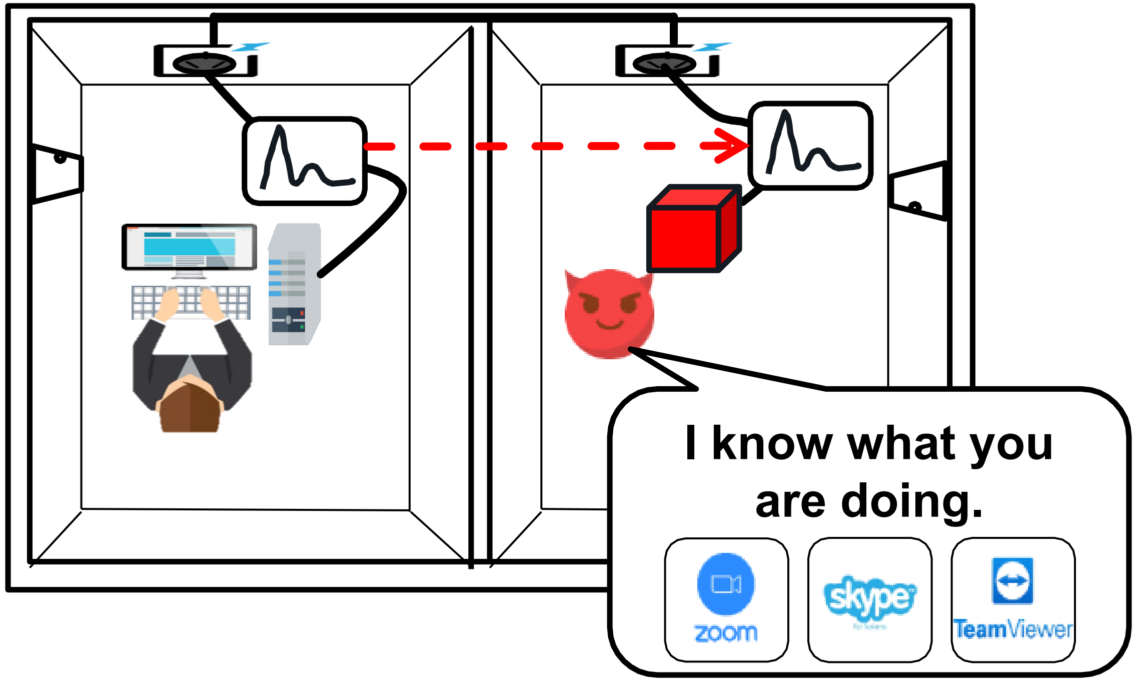


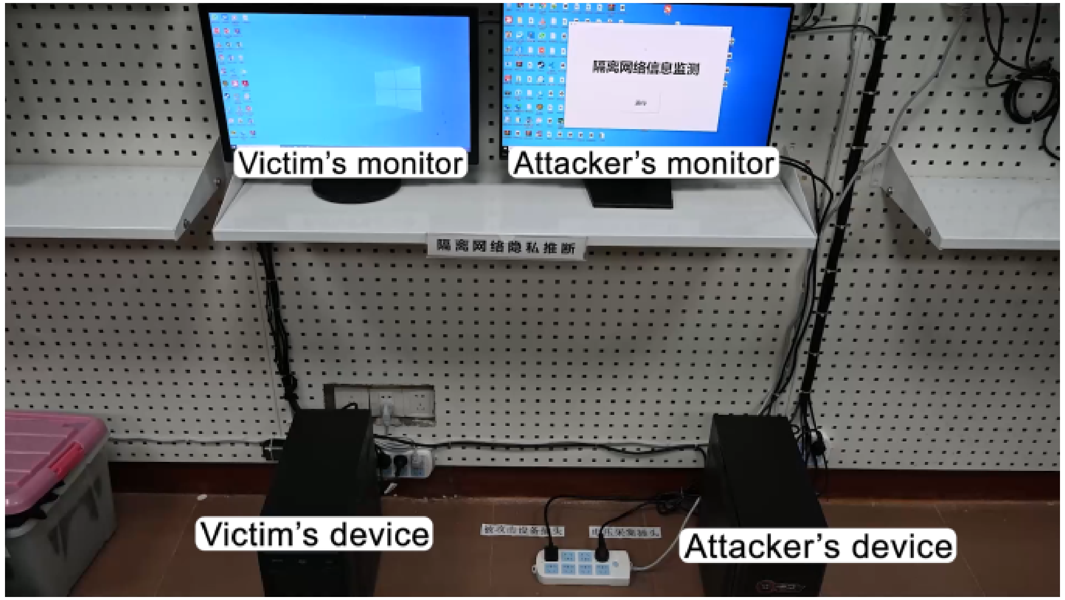
RF signal

Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. “Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers.” CCS '18

4.2 Side Channel: App State→ Power Cable Signal

Side channel application working state → power cable signal



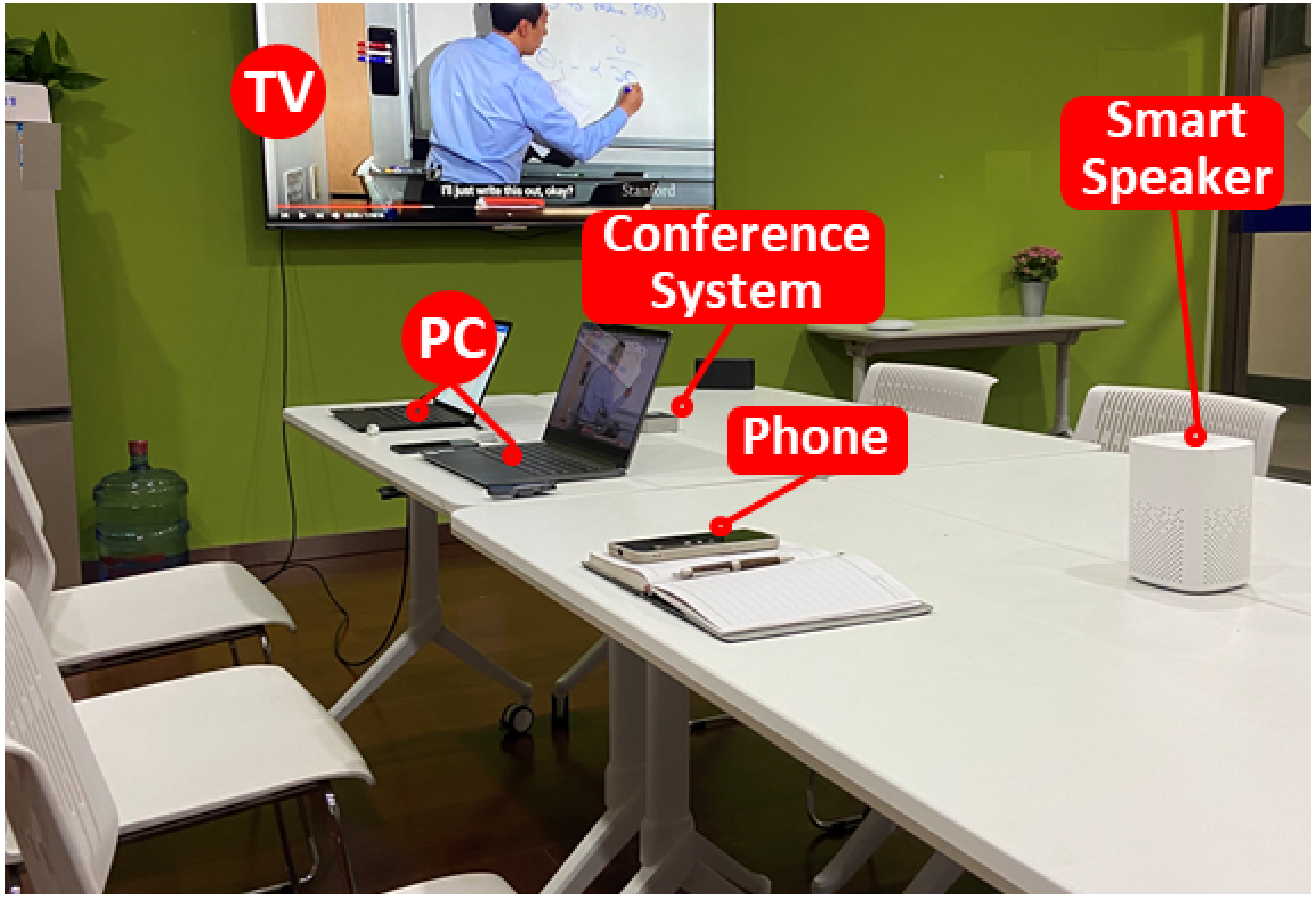


Juchuan Zhang, Xiaoyu Ji, Yuehan Chi, Yi-chao Chen, Bin Wang, and Wenyuan Xu. "OutletSpy: Cross-outlet Application Inference via Power Factor Correction Signal," ACM WiSec 2021

4.3 Side Channel: Voice Recorders → ADC EM Radiation

- How to detect voice recorder?

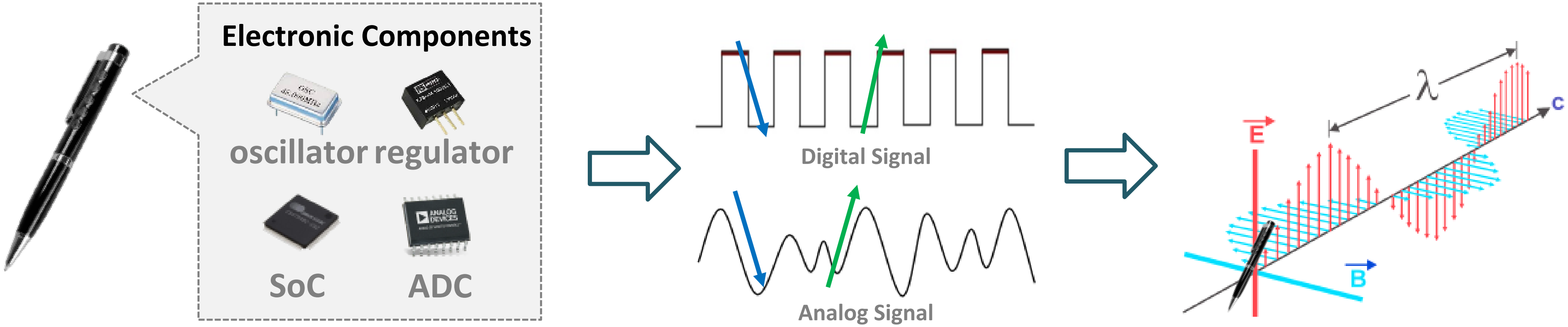
- Using the side channel of EM radiation



Ruochen Zhou, Xiaoyu Ji, Chen Yan, Yi-chao Chen, Wenyuan Xu, and Chaohao Li. "DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation," S&P 2023

4.3 Side Channel: Voice Recorders → ADC EM Radiation

- Identify an offline recorder by measuring its EMR



Electronic Components

oscillator regulator

SoC ADC

Digital Signal

Analog Signal

Recorder

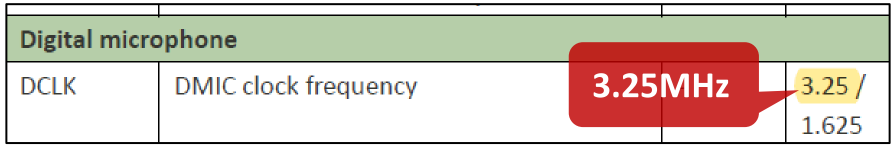
Varying Current

EMR

4.3 Side Channel: Voice Recorders → ADC EM Radiation

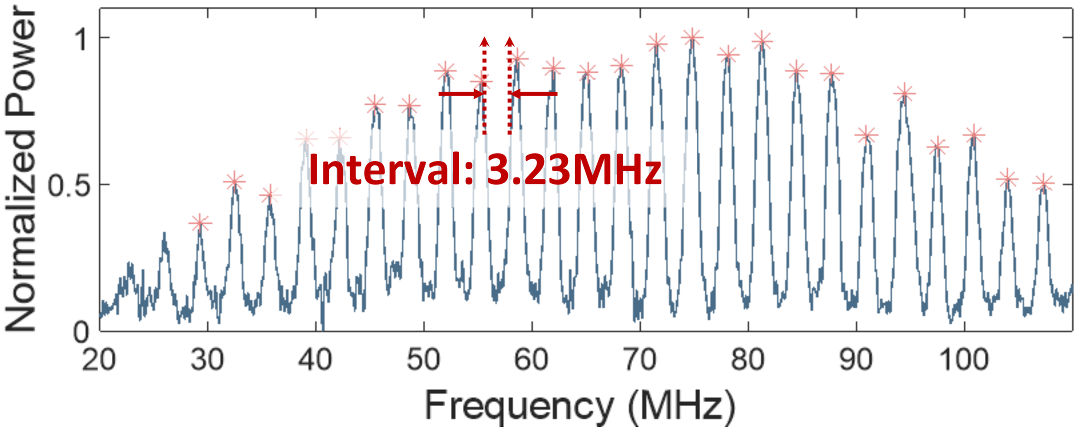
- **Unique pattern of EMI radiated by ADC**

Sogou C1

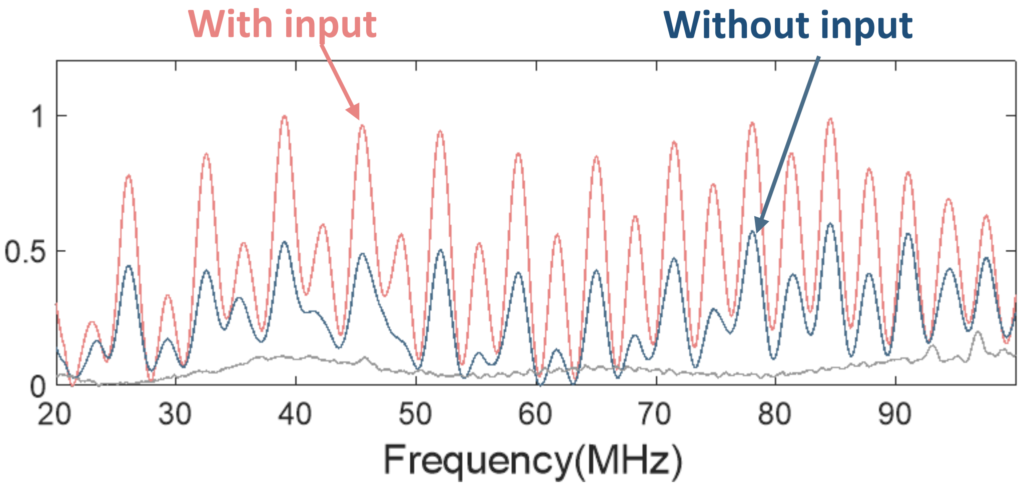


Digital microphone			
DCLK	DMIC clock frequency		3.25 / 1.625

3.25MHz



ADC pattern of Sogou C1

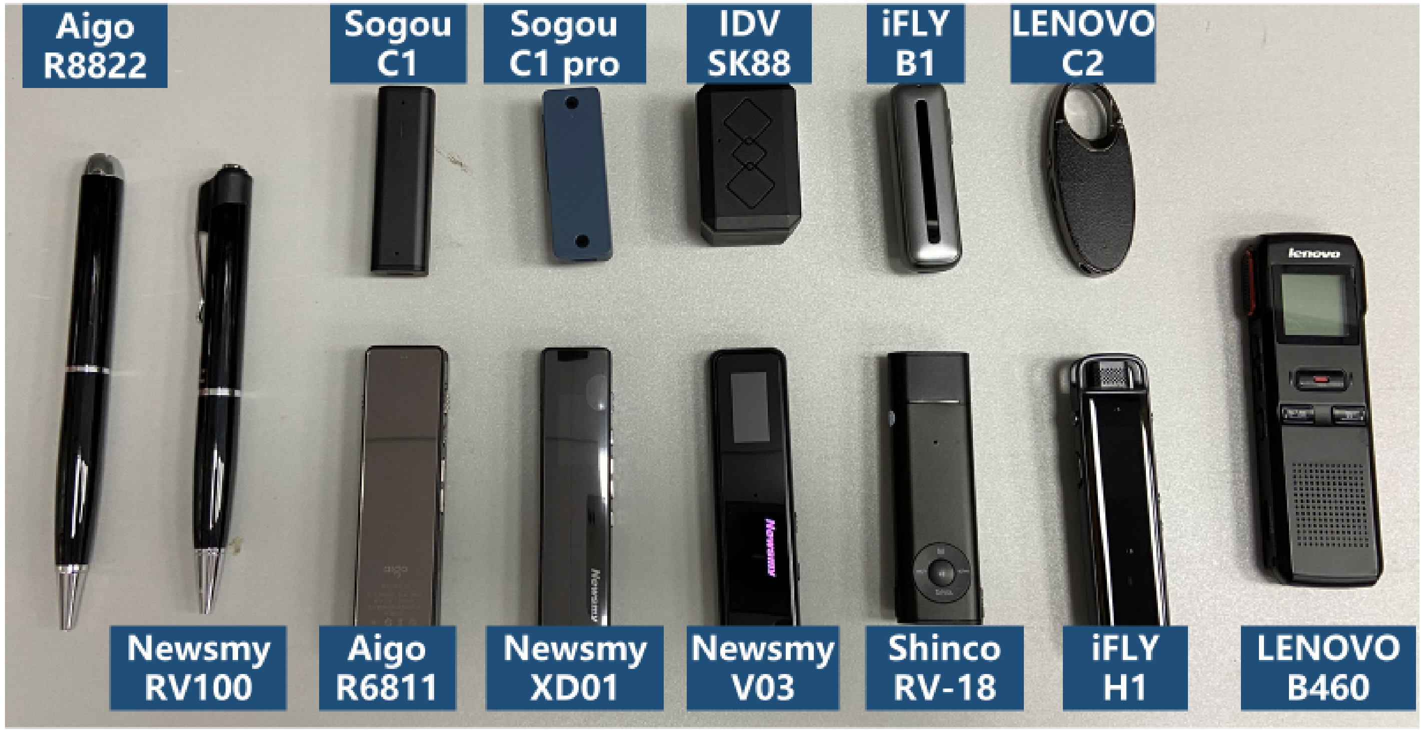


With and without input

Ruochen Zhou, Xiaoyu Ji, Chen Yan, Yi-chao Chen, Wenyuan Xu, and Chaohao Li. "DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation," S&P 2023

4.3 Side Channel: Voice Recorders → ADC EM Radiation

- Overall recorders detection accuracy is 92.17% with a Recall of 86.14%
- Average True Negative Rate for 21 interfering devices is 95.05%



Targeted recorders

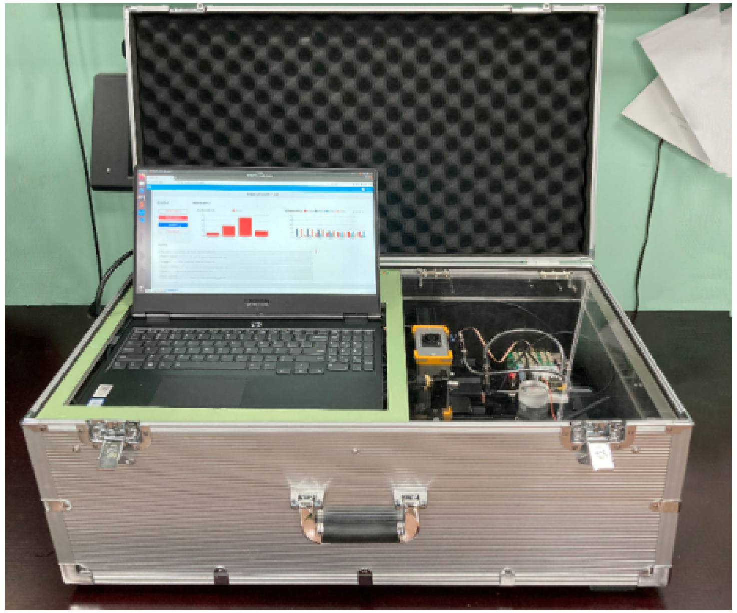
Interfering devices

How to **DETECT** and **MITIGATE** out-of-band vulnerabilities?

Out-of-Band Vulnerability Scanning Toolkit

- Automates the detection of **over-limit signal** and **cross-sensing** vulnerabilities.
- **Discovered 10+ new vulnerabilities in sensors** including cameras, LiDAR, microphones, accelerometers, etc.

OOB Scanning Toolkit



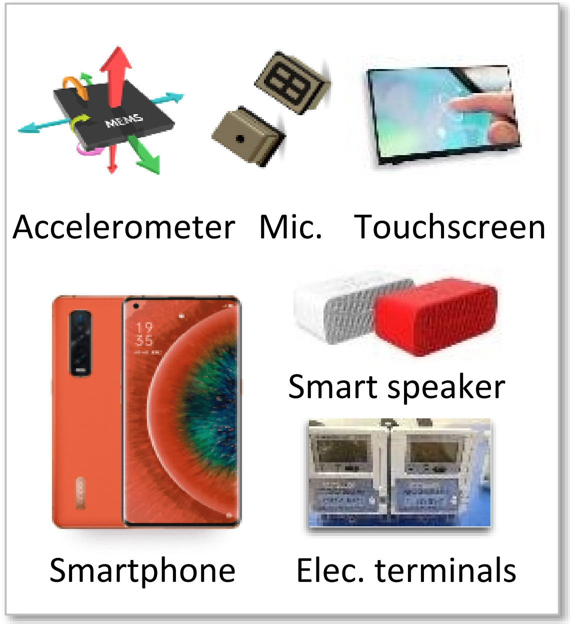
Application

Application 1：
Autonomous Vehicle

Camera LiDAR Radar

Autonomous Vehicle

Application 2：
Internet of Things



Accelerometer Mic. Touchscreen

Smart speaker

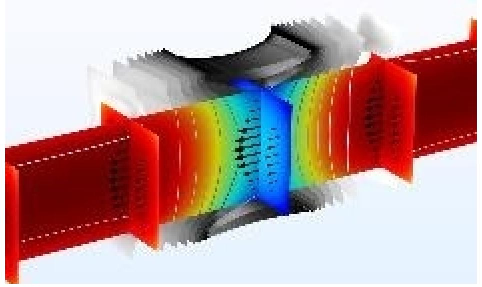
Smartphone Elec. terminals

Mitigating Out-of-Band Security Threat

- **Solution 1:** Eliminate out-of-band vulnerabilities from system design
- **Solution 2:** Usable attack detection and prevention

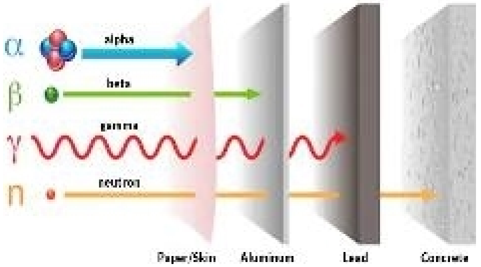
Solution 1

Module Fidelity Design



Match ideal design with non-ideal characteristics

Signal Filtering & Shielding



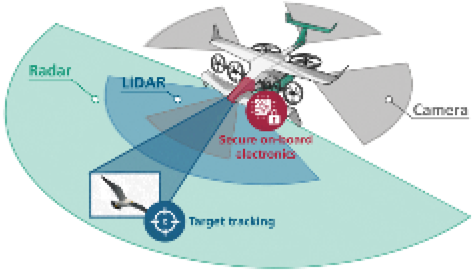
Filter over-limit signals
Shield cross-field signals

Solution 2

Attack Detection & Elimination

Identify and intercept attacks

System Robustness Enhancement



Fuse information and enhance robustness

Future work

How to cope with Out-of-band vulnerabilities?

Promote research on:

- Out-of-band **theory** and root cause
- Quantitative **analysis and detection**
- Systematic **defense** without affecting in-band functions
- Open **platform for cross-domain research**

Summary

- Balance ‘in-band’ and **‘out-of-band’ vulnerability**
- Integrated spectrum signal security **risks**
  - RF, Acoustic, Lightwave…
- **Testing is important！**
  - Systematically exploit vulnerability
  - Fuzzy testing takes into account both in-band and out-of-band

We committed to making the IOT more secure！

Thanks

Email: xji@zju.edu.cn
HOME PAGE： http://www.usslab.org