Introduction to IoT & Embedded Security

Yan Long
yan.long@virginia.edu | yanlong.site

Northeastern University & University of Virginia

Objectives & Outline

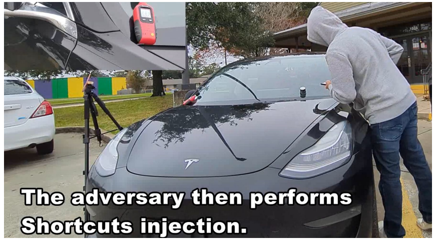
- What are embedded/IoT security?
- Some examples.
- Grand challenges & future research topics?

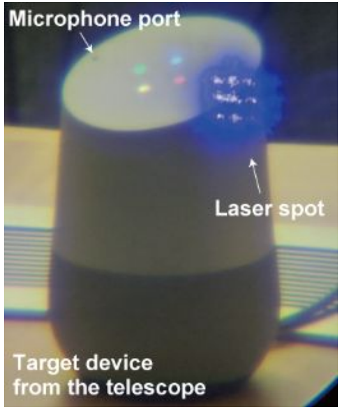
Objectives & Outline

- What are embedded/IoT security?
- Some <u>examples</u>.
- Grand challenges & future research topics?

<u>examples</u>

- Smart cards
- Networked cameras
- Medical devices
- Laser injection into mics (Demo)
- Optical-acoustic side channel
- Camera EM leakage (Demo)
- Car hijacking in IoT automation





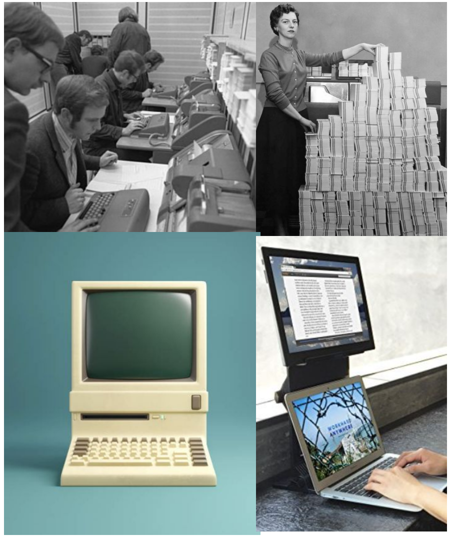
Embedded Security?

what is embedded/IoT security ≈ what is an embedded/iot system

[Photo: Amazon, Apple,Samsung, Emotiv, NPR]

Embedded Systems

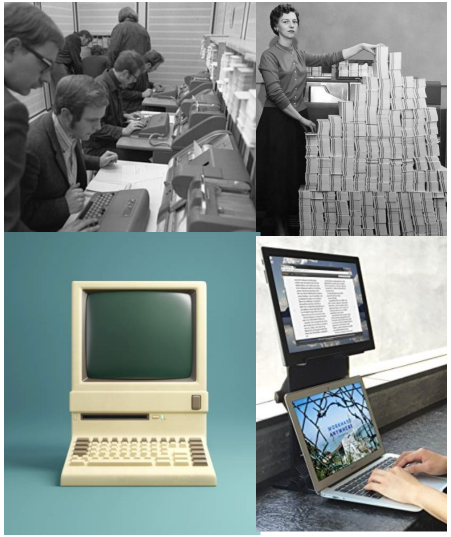
Conventional Computer Systems



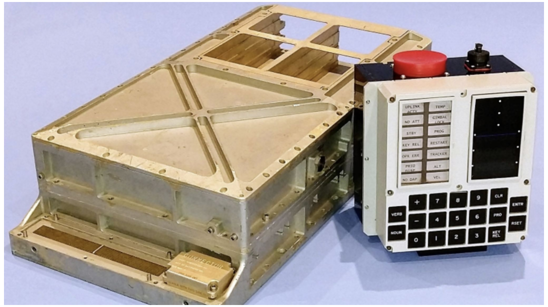
Embedded Systems

Let's use computers on other devices!

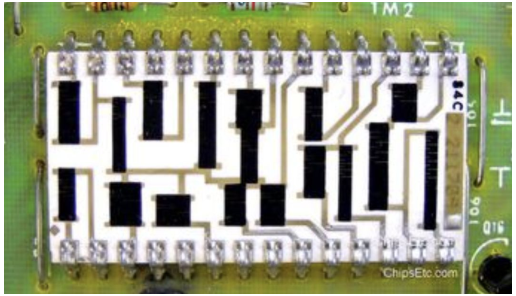
Conventional Computer Systems



MCUs in Apollo spacecrafts in 1960s



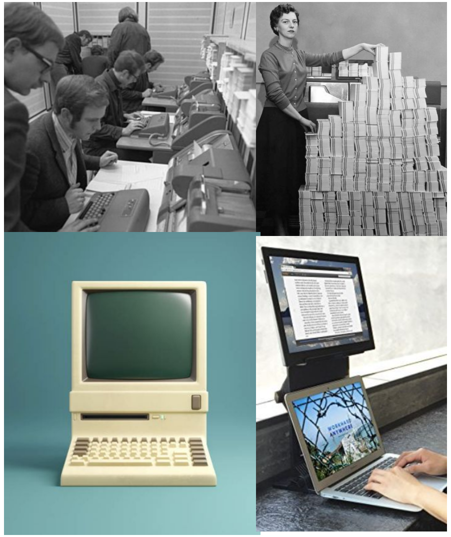
ECUs in cars in 1970s



Embedded Systems

Turn everything into computers!

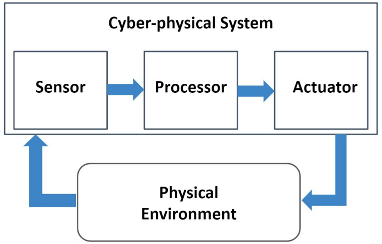
Conventional Computer Systems

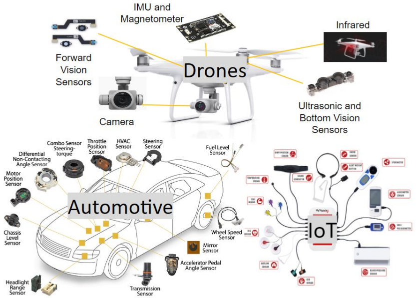


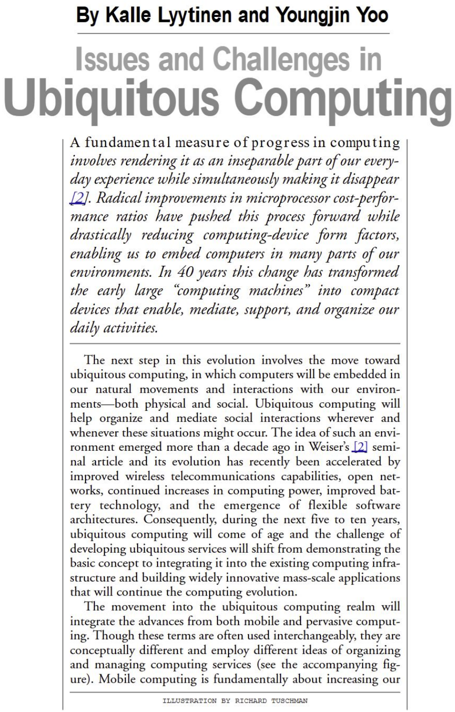
Sensing, Actuation

Embedded Form

Embedded Systems






By Kalle Lyytinen and Youngjin Yoo

Issues and Challenges in
Ubiquitous Computing

A fundamental measure of progress in computing *involves rendering it as an inseparable part of our everyday experience while simultaneously making it disappear [2]. Radical improvements in microprocessor cost-performance ratios have pushed this process forward while drastically reducing computing-device form factors, enabling us to embed computers in many parts of our environments. In 40 years this change has transformed the early large "computing machines" into compact devices that enable, mediate, support, and organize our daily activities.*

The next step in this evolution involves the move toward ubiquitous computing, in which computers will be embedded in our natural movements and interactions with our environments—both physical and social. Ubiquitous computing will help organize and mediate social interactions wherever and whenever these situations might occur. The idea of such an environment emerged more than a decade ago in Weiser's [2] seminal article and its evolution has recently been accelerated by improved wireless telecommunications capabilities, open networks, continued increases in computing power, improved battery technology, and the emergence of flexible software architectures. Consequently, during the next five to ten years, ubiquitous computing will come of age and the challenge of developing ubiquitous services will shift from demonstrating the basic concept to integrating it into the existing computing infrastructure and building widely innovative mass-scale applications that will continue the computing evolution.

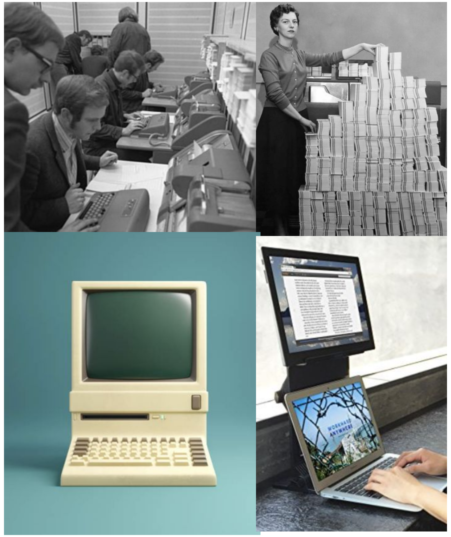
The movement into the ubiquitous computing realm will integrate the advances from both mobile and pervasive computing. Though these terms are often used interchangeably, they are conceptually different and employ different ideas of organizing and managing computing services (see the accompanying figure). Mobile computing is fundamentally about increasing our

ILLUSTRATION BY RICHARD TUSCHMAN

IoT Systems

Finally, connect them all :)

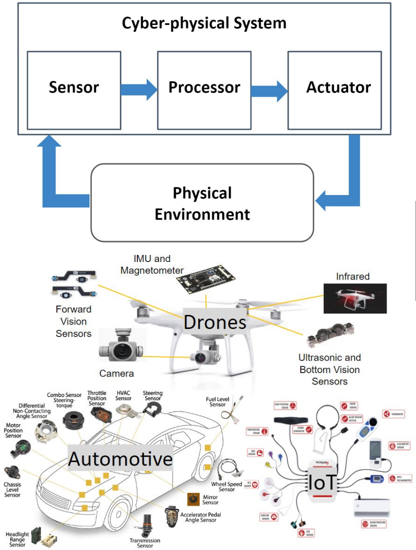
Conventional Computer Systems



Sensing, Actuation

Embedded Form

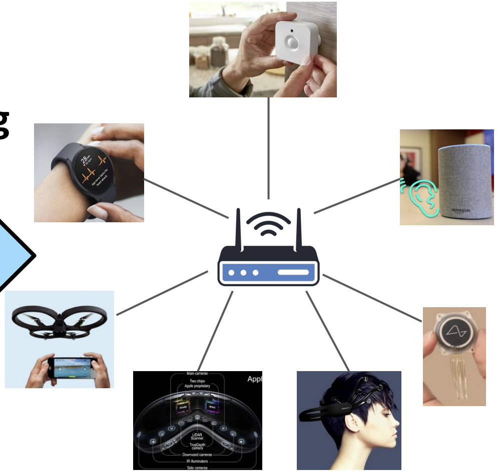
Embedded Systems



Networking

Connected Form

IoT Systems



Unique Properties

- Frequent direct exposure to physical environments (physics)
- Sensing and actuation
- Limited user-machine interactions
- Miniaturized low-resource devices
- Huge amount of connected devices and data

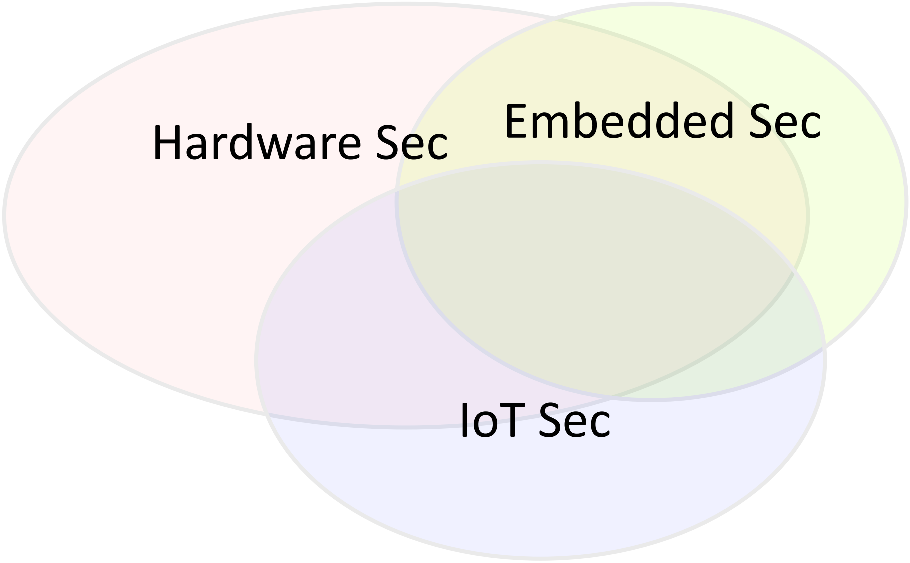
Unique Properties

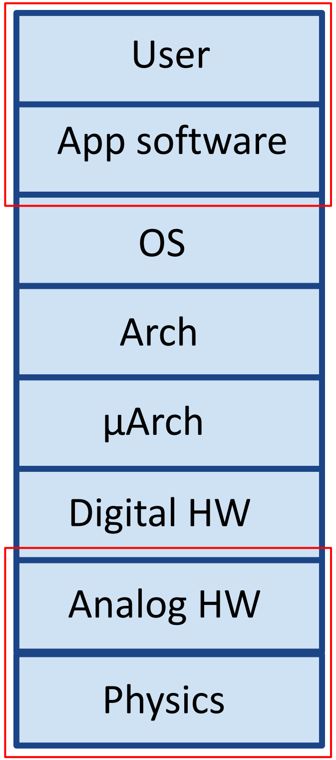
- Frequent direct exposure to physical environments (physics)
- Sensing and actuation
- Limited user-machine interactions
- Miniaturized low-resource devices
- Huge amount of connected devices and data

→ Unique Security Problems?

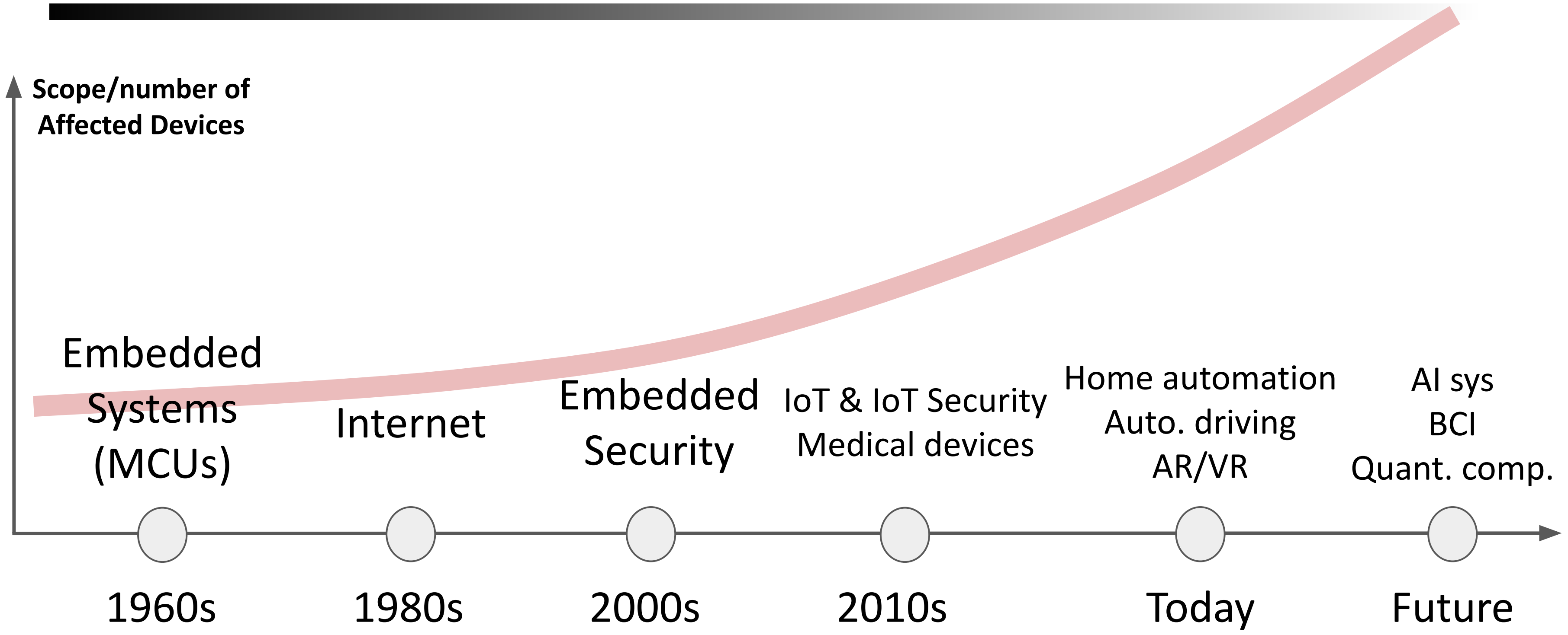
Unique Problems

Security research finds flaws in the abstraction.

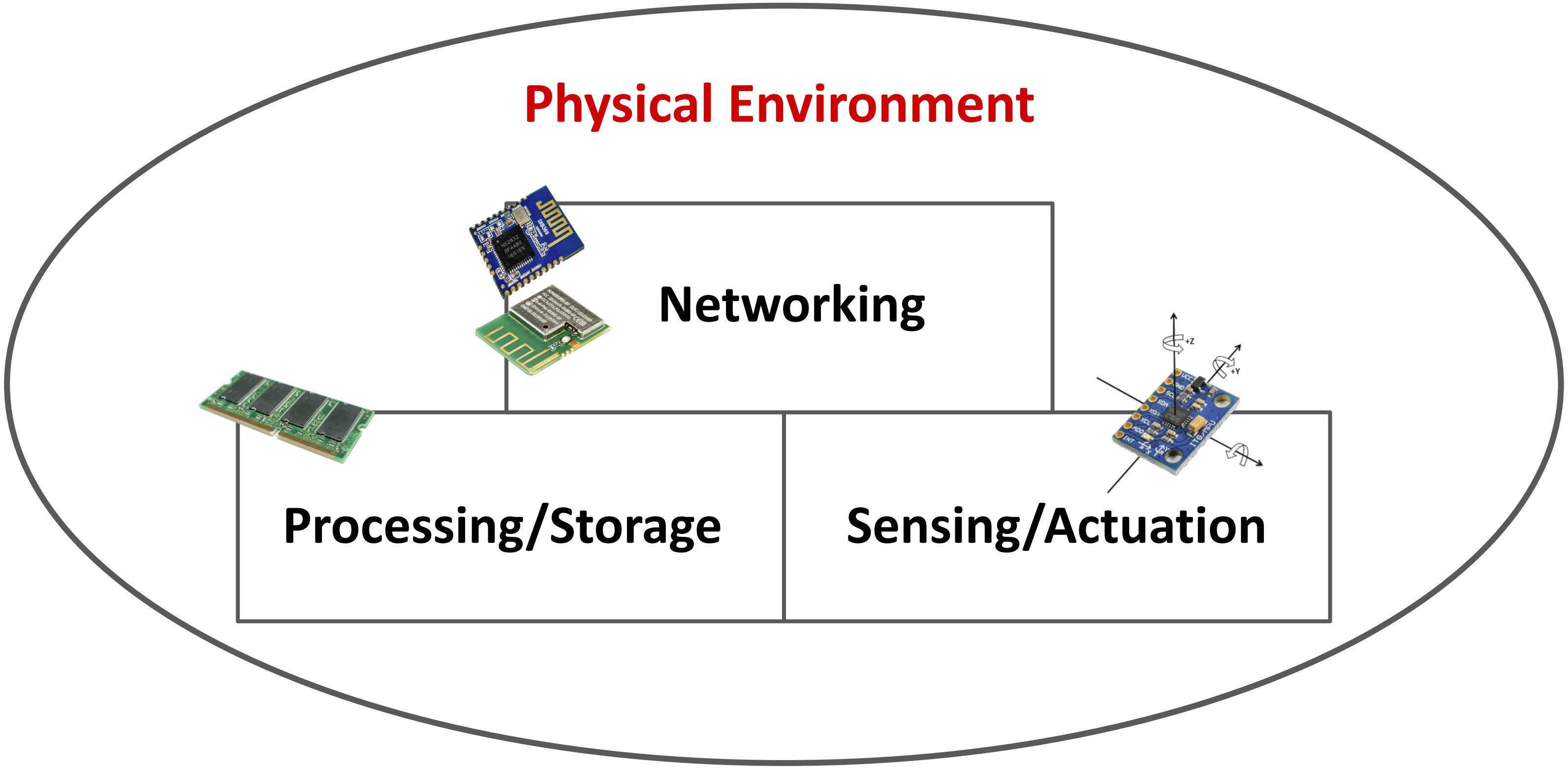




Some History

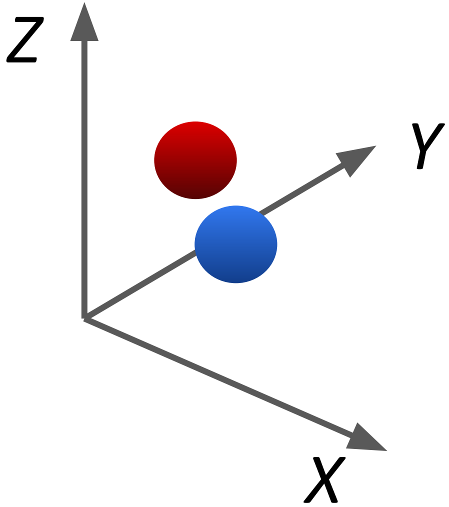


Embedded IoT Sys Building Blocks

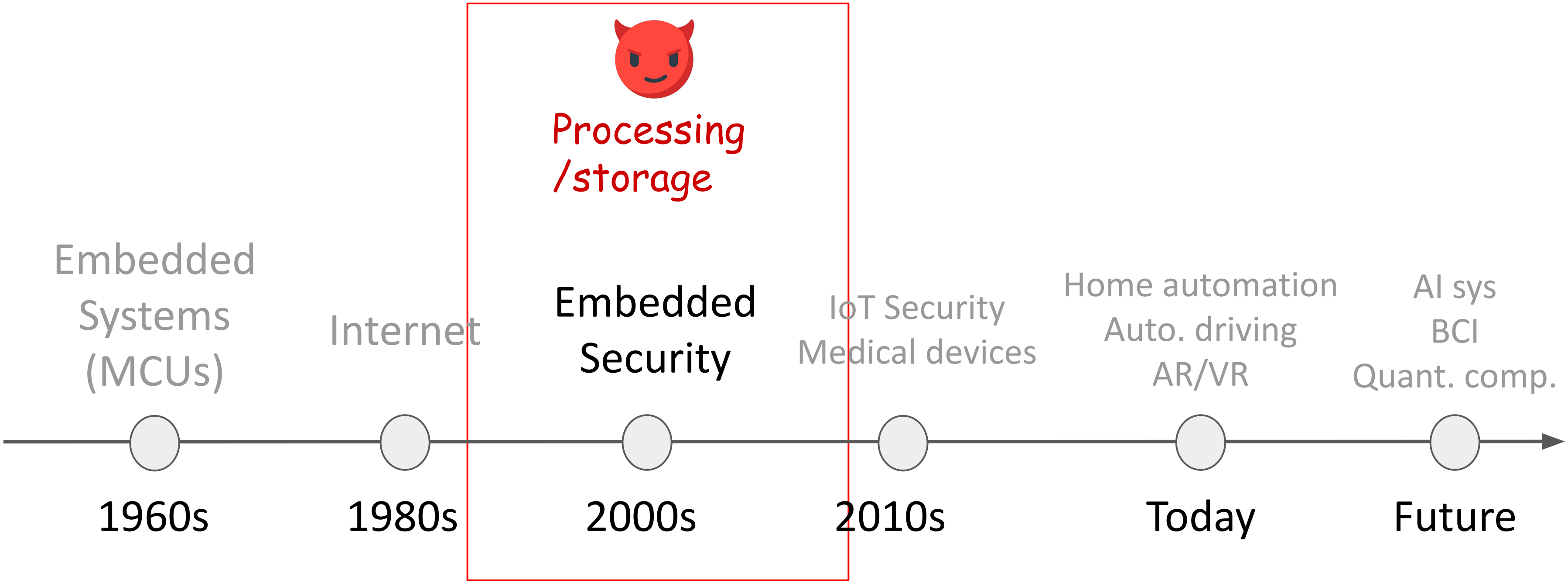


A Rough Taxonomy

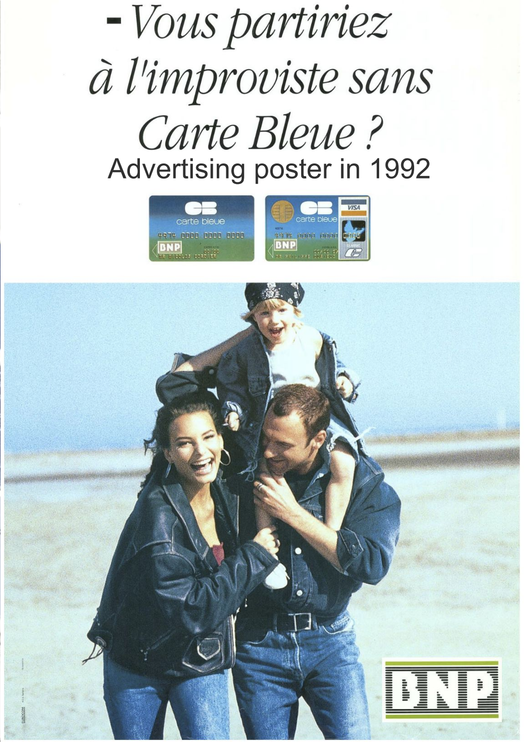
- Time (when it happened => why it was possible)
- System component (where did this happen)
- Abstraction gap (how does it work)



Timeline


Processing
/storage
Embedded
Systems
(MCUs)
Internet
Embedded
Security
IoT Security
Medical devices
Home automation
Auto. driving
AR/VR
AI sys
BCI
Quant. comp.
1960s
1980s
2000s
2010s
Today
Future

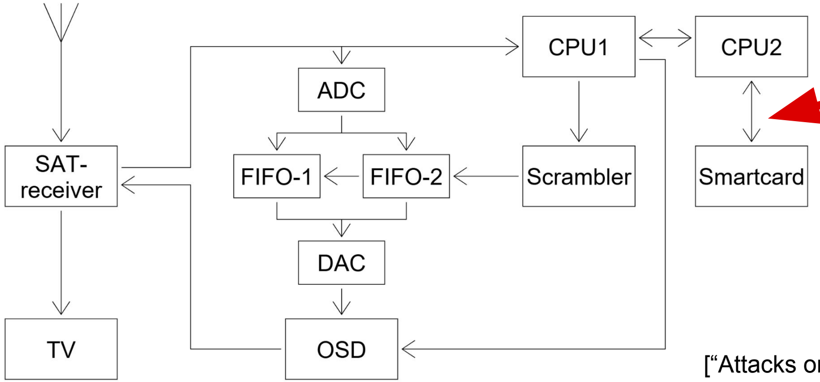
Smart Cards

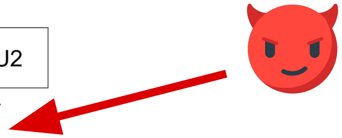


Advertising poster in 1992

[Source: Wiki, BNP]

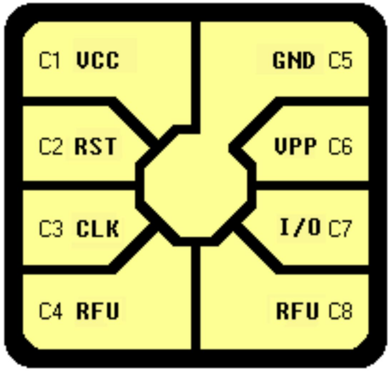
Smart Cards: Pay-TV Hacking





[“Attacks on Pay-TV Access Control Systems”, Markus Kuhn, 1997]

Smart Cards: Power Analysis



VCC= Power

VPP= Programming Voltage

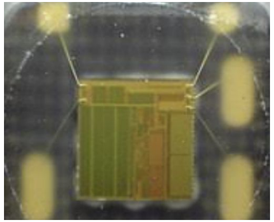
RFU= Reserved for future use

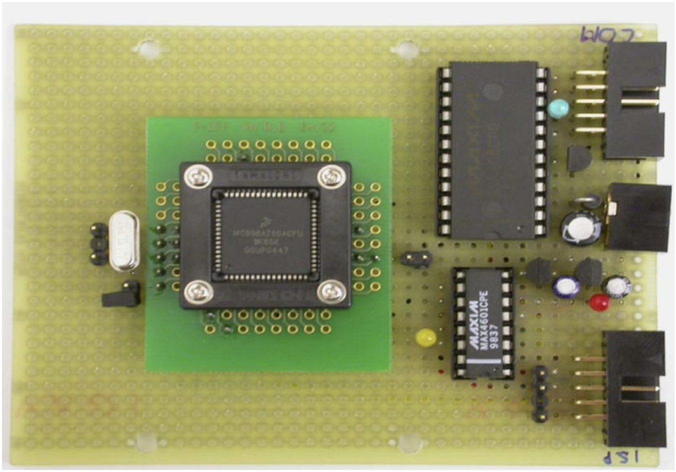
I/O= Input/Output

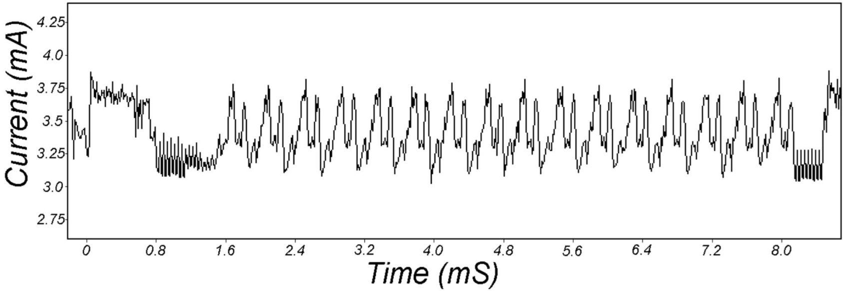
CLK= Clock

RST= Reset

GND= Ground



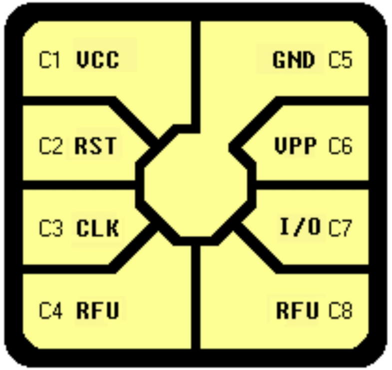




[“Differential Power Analysis”, Kocher et al., 1999]

[“Breaking Smartcards Using Power Analysis”, Choudary, 2005]

Smart Cards: Fault Injection



VCC= Power

VPP= Programming Voltage

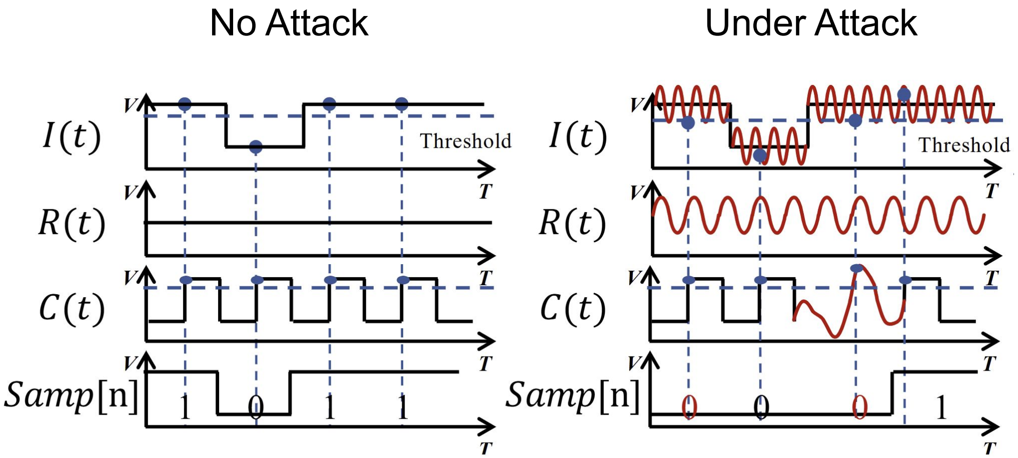
RFU= Reserved for future use

I/O= Input/Output

CLK= Clock

RST= Reset

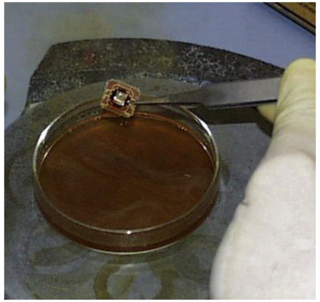
GND= Ground

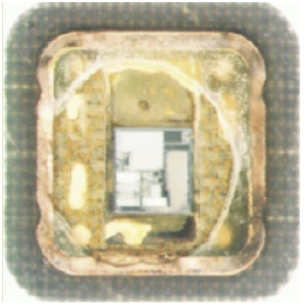


Laser/EM Fault Injection

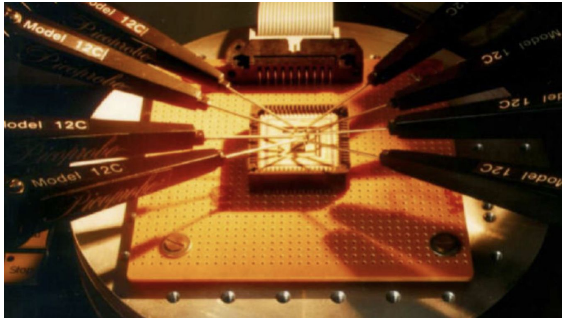
Smart Cards: Invasive Probing

Extracting chips from smart cards

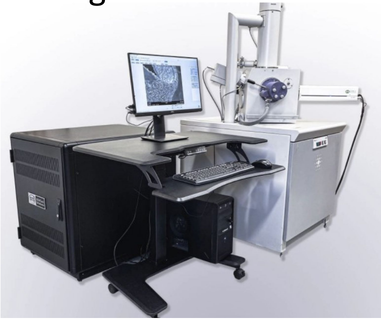




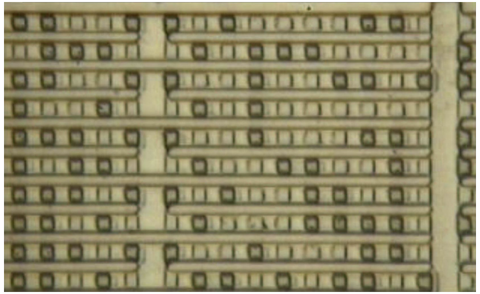
Probing with physical needle or electron beams



Scanning Electron Microscope



Imaging & reading ROM content

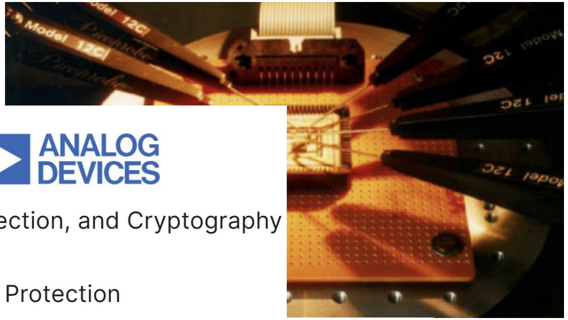


[Source: Erik Pol, Oliver Kömmerling, Marcus Kuhn, SEMTech Solutions]

Tamper-resistant Hardware

Extracting chips from smart cards | Probing with physical needle or electron beams





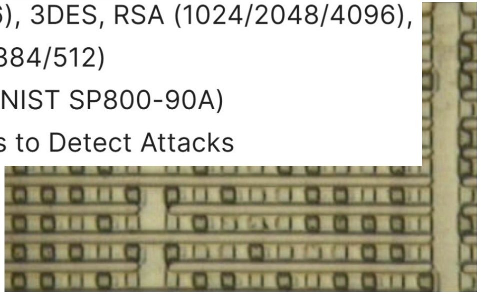
MAX36210 PRODUCTION ⓘ ANALOG DEVICES

Security Supervisor with SP800-90A TRNG, Tamper Detection, and Cryptography

Small Footprint, Secure Memory with Advanced Security Protection

- Security Features Facilitate System-Level Protection
  - Tamper Detection with Fast Wipe Key/Data Destruction
  - Hardware Accelerators for AES (128/192/256), 3DES, RSA (1024/2048/4096), ECDSA (p256/p384/p521), SHA (1/224/256/384/512)
  - True Hardware Random-Number Generator (NIST SP800-90A)
  - Temperature, Voltage and Die Shield Sensors to Detect Attacks

Sc… …ntent

[Source: Erik Pol, Oliver Kömmerling, Marcus Kuhn, SEMTech Solutions]

Timeline

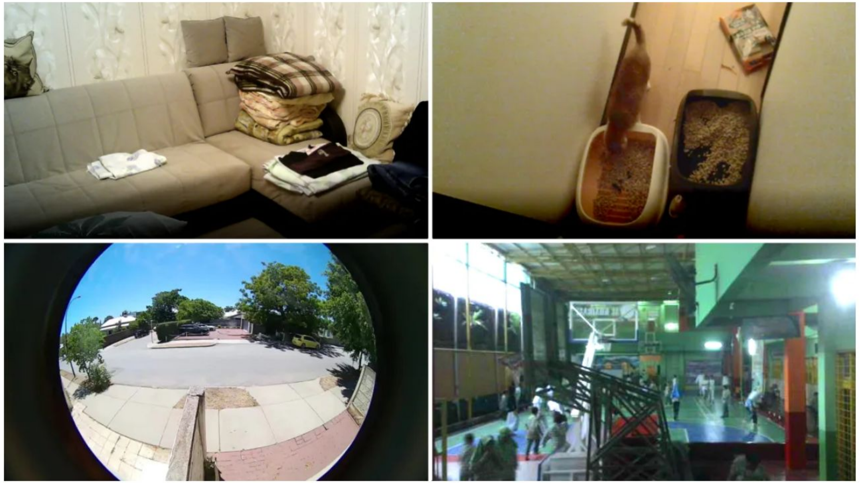
Networking

1960s	1980s	2000s	2010s	Today	Future
Embedded Systems (MCUs)	Internet	Embedded Security	IoT Security Medical devices	Home automation Auto. driving AR/VR	AI sys BCI Quant. comp.

IP Camera Hijacking

‘Internet of things’ or ‘vulnerability of everything’? Japan will hack its own citizens to find out

By James Griffiths, CNN
5 minute read · Published 9:59 PM EST, Fri February 1, 2019



Shodan
https://www.shodan.io
Shodan Search Engine

Insecam - Live cameras directory
(>100,000 live cams)

Start browsing popular online cams >>>

Live camera in Iiyama, Japan

Live camera in Minden, Germany

Live camera in Porirua, New Zealand

POLITICS ENTERTAINMENT LIFE PARENTS COST OF LIVING SHOPPING

TECH INSECAM WEBCAM WEBCAM SECURITY

Insecam Webcam Site Creator: 'I'm Not Sorry. And MY Cameras Were On My Site Too'

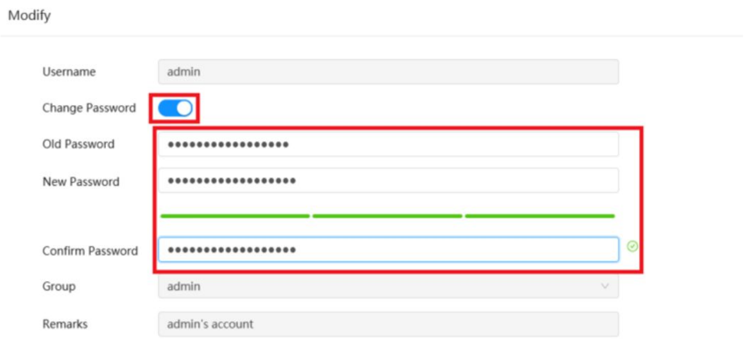
'I'm Not Sorry' Webcam 'Spy' Hacker Tells HuffPost

Michael Rundle — The Huffington Post UK

25/11/2014 03:41am GMT | **Updated** November 25, 2014

But why?

- Users:
  - What is password?
  - Why do I need to change it?
  - What the heck is internet?
- Designers:
  - Our UIs suck.
  - Our manuals suck.
  - Our security guidance == None



Hijacking Other Devices for DDoS

WIRED

The Mirai Botnet Architects Are Now Fighting Crime With the FBI

In 2016 three friends created a botnet that nearly broke the internet. Now, they're helping the feds catch cybercriminals of all stripes.

Infected IoT devices (>600,000)

- Cameras
- Printers
- Routers
- TVs
- Network-Attached Storage Devices
- ……

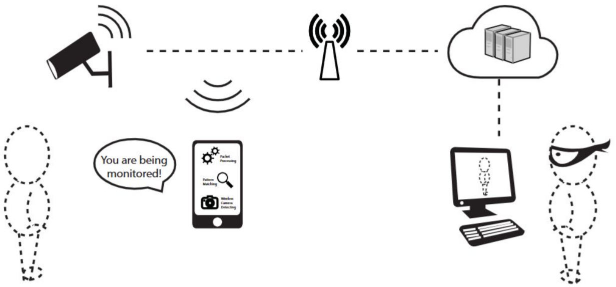
[“Understanding the Mirai Botnet”, Antonakakis et al., USENIX Security 2017]

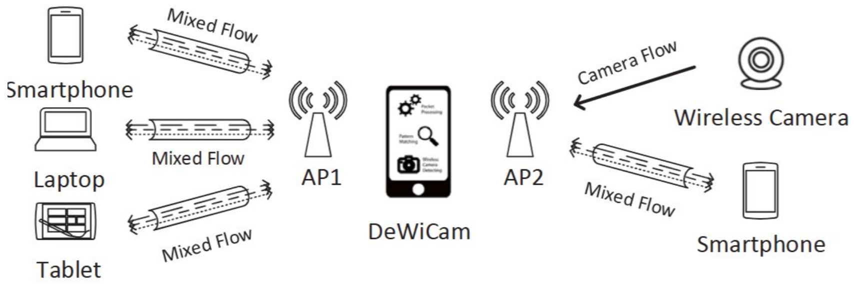
Detecting Hidden Cameras

Session 1: Embedded System Security ASIACCS'18, June 4–8, 2018, Incheon, Republic of Korea

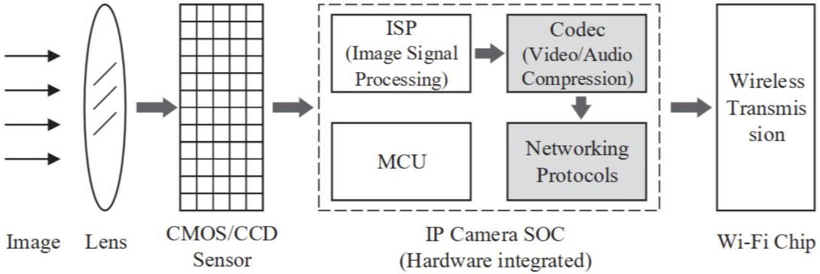
DeWiCam: Detecting Hidden Wireless Cameras via Smartphones

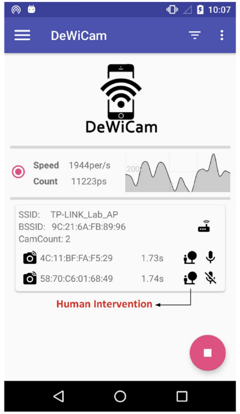
Yushi Cheng[1,2], Xiaoyu Ji[1,2†], Tianyang Lu[1], Wenyuan Xu[1†]
[1] Ubiquitous System Security Lab (USSLAB), Zhejiang University
[2] Alibaba-Zhejiang University Joint Institute of Frontier Technologies
Emails: {yushicheng, xji, 5pipi, wyxu}@zju.edu.cn

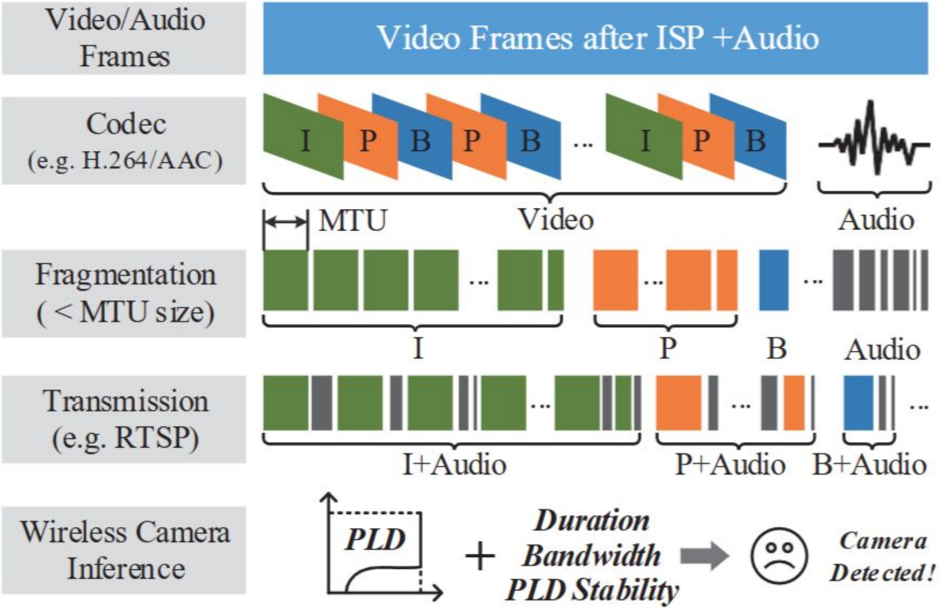




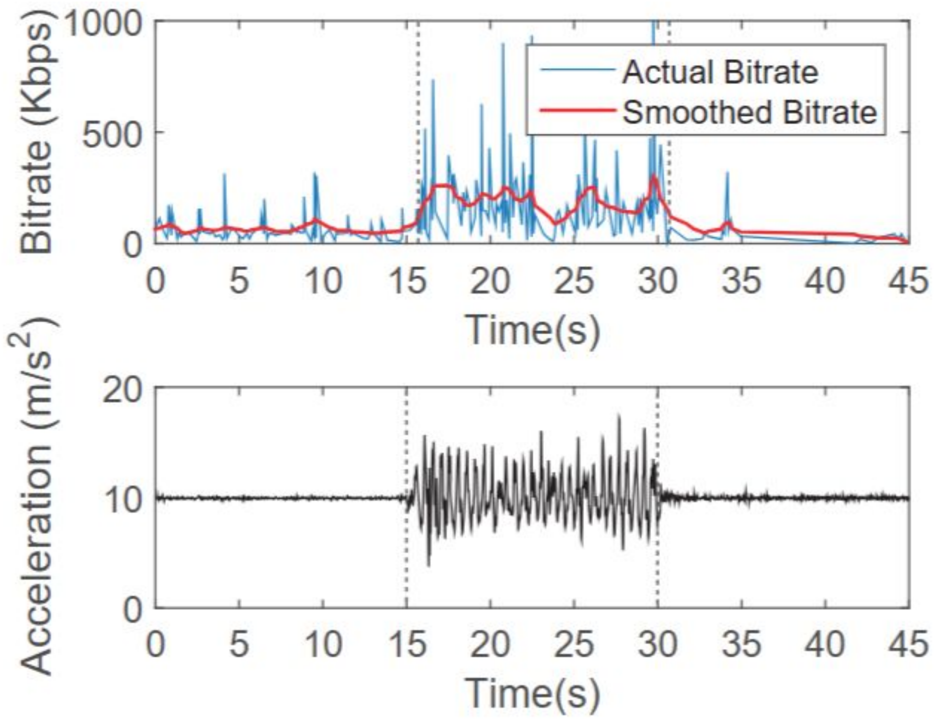
Detecting Hidden Cameras







Detecting Hidden Cameras



OPPO Introduces Hidden Camera Detection in ColorOS 12.1

Mar 15, 2022 07:45 OnePlus Community 87 51 11.8k

Detecting Hidden Cameras

ACM CCS'22

HeatDeCam: Detecting Hidden Spy Cameras via Thermal Emissions

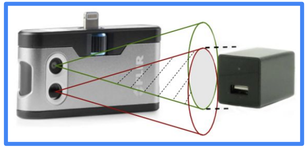
Zhiyuan Yu
Washington University in St. Louis
St. Louis, USA
yu.zhiyuan@wustl.edu

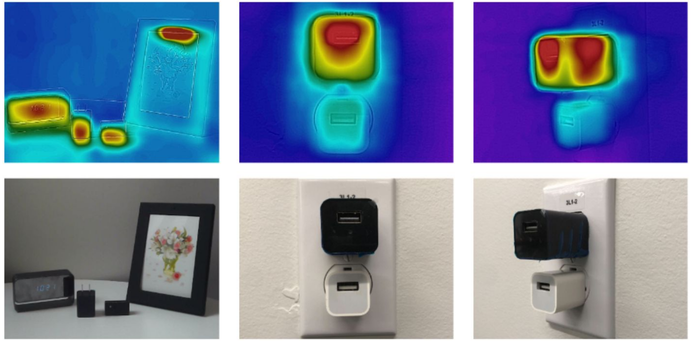
Zhuohang Li
University of Tennessee, Knoxville
Knoxville, USA
zli96@vols.utk.edu

Yuanhaur Chang
Washington University in St. Louis
St. Louis, USA
c.yuanhaur@wustl.edu

Jian Liu
University of Tennessee, Knoxville
Knoxville, USA
jliu@utk.edu

Ning Zhang
Washington University in St. Louis
St. Louis, USA
zhang.ning@wustl.edu





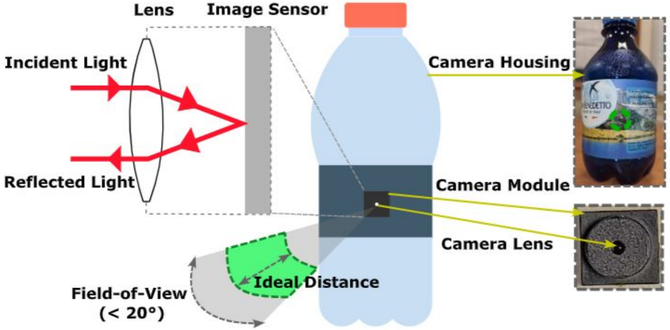
ACM SenSys'21

LAPD: Hidden Spy Camera Detection using Smartphone Time-of-Flight Sensors

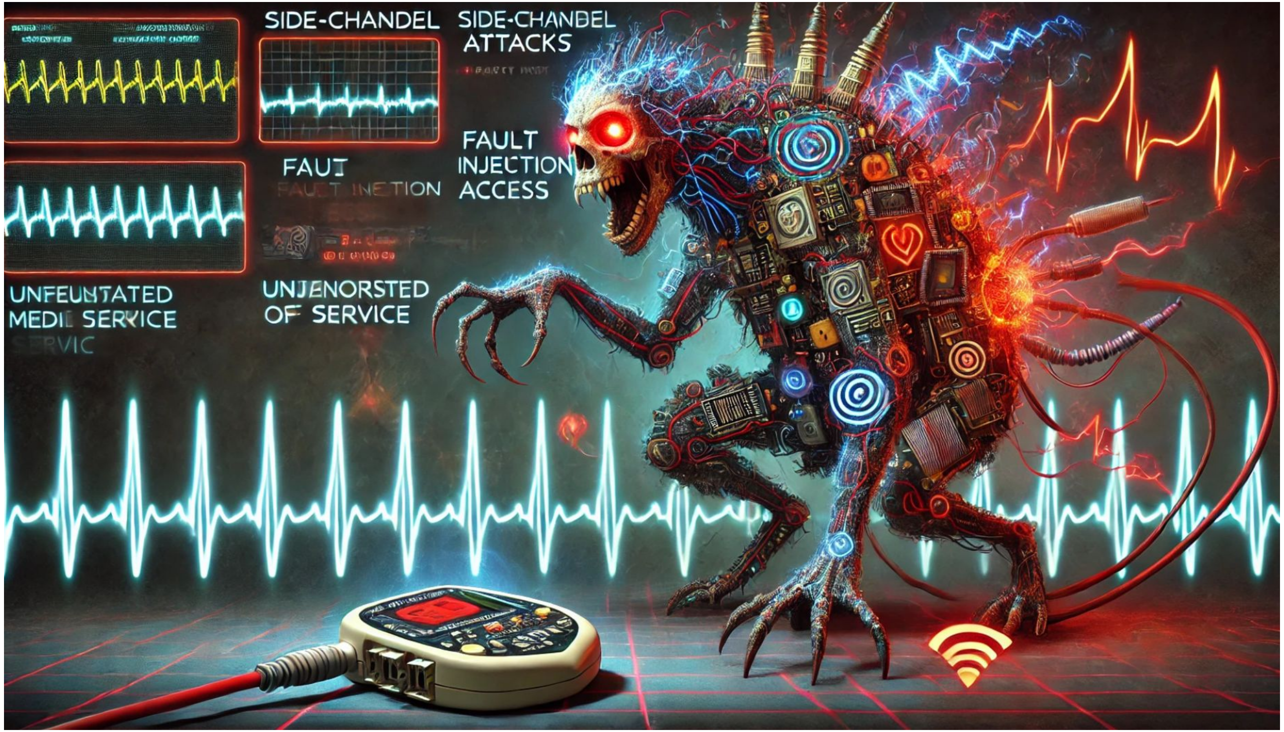
Sriram Sami
National University of Singapore

Sean Rui Xiang Tan
National University of Singapore
seantanr@comp.nus.edu.sg

Jun Han*
Yonsei University
jun.han@yonsei.ac.kr



Medical Device Security



[Graph by ChatGPT]

Implantable Devices

IEEE S&P'08

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin†
University of Washington

Thomas S. Heydt-Benjamin†
University of Massachusetts Amherst

Benjamin Ransford†
University of Massachusetts Amherst

Shane S. Clark
University of Massachusetts Amherst

Benessa Defend
University of Massachusetts Amherst

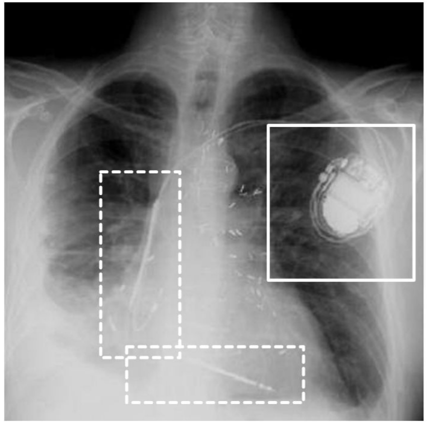
Will Morgan
University of Massachusetts Amherst

Kevin Fu, PhD*
University of Massachusetts Amherst

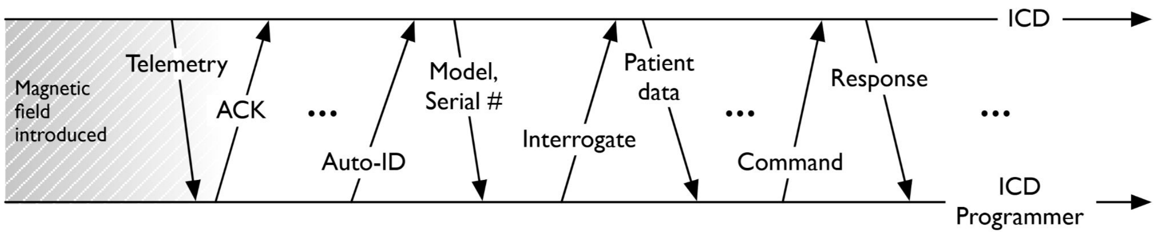
Tadayoshi Kohno, PhD*
University of Washington

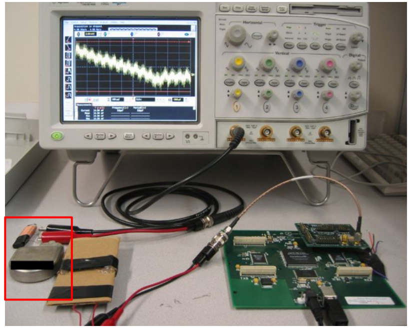
William H. Maisel, MD, MPH*
BIDMC and Harvard Medical School

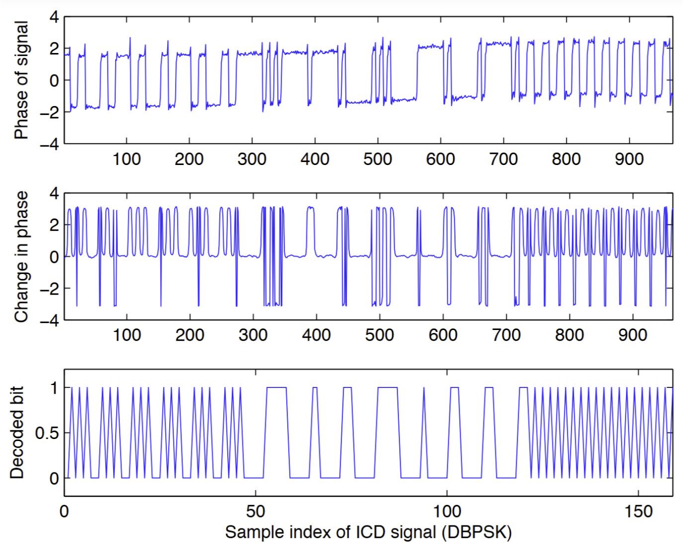
Broken Hearts (*Homeland*)



Implantable Devices







Insulin Pumps

2011 IEEE 13th International Conference on e-Health Networking, Applications and Services

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System

Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

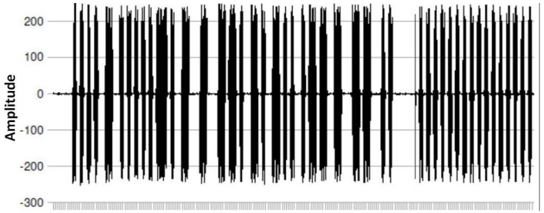
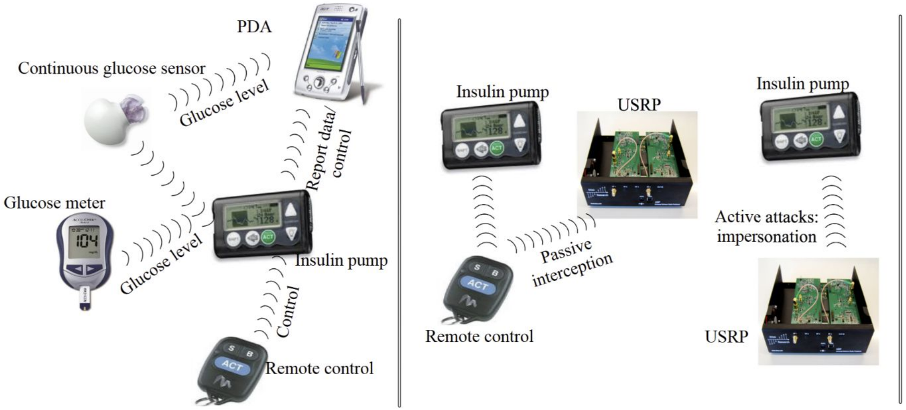


Fig. 2. Signal intercepted by USRP



RFID Security

Card Not Present Fraud , Fraud Management & Cybercrime

Criminals 'Ghost Tap' NFC for Payment Cash-Out Attacks

BANKINFO SECURITY

Tactic Uses Stolen Cards Added to Apple Pay and Google Pay Digital Wallets

Mathew J. Schwartz (euroinfosec) • November 20, 2024

Digital Security

To tap or not to tap: Are NFC payments safer?

Contactless payments are quickly becoming ubiquitous – but are they more secure than traditional payment methods?

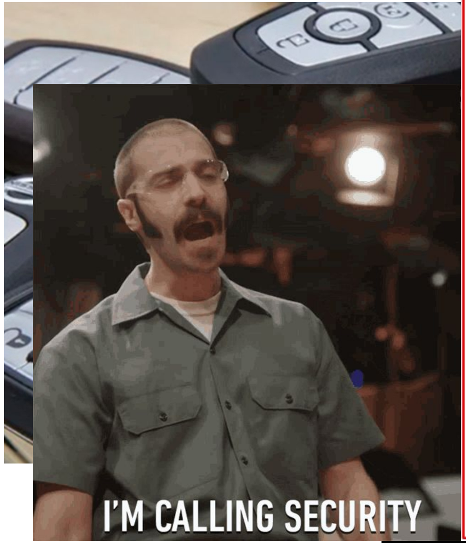
Márk Szabó

TECHNOLOGY

One Tech Tip: Protecting your car from the growing risk of keyless vehicle thefts

AP

RFID Security



Forget tin foil. Put your keys in the fridge to keep them safe from car thieves

USA TODAY

Kim Komando Special for USA TODAY

Published 9:53 a.m. ET Aug. 10, 2018 | **Updated 3:35 p.m. ET Aug. 10, 2018**

Steps to stop car thieves

There are a few easy ways to block criminals' amplified signals. You can buy a signal-blocking pouch that can hold your keys, such as a shielded RFID blocking pouch.

- **Stick in the fridge:** The free option is to use your refrigerator or freezer. The multiple layers of metal will block your key fob's signal. Just check with the fob's manufacturer to make sure freezing your key fob won't damage it.
- **Place in your microwave oven:** If you're not keen to freeze your key fob, you can do the same thing with your microwave oven. The metal frame should work as well as your refrigerator. Here, though, it's vital that you don't turn your microwave on, as you could cause serious damage and even start a fire.
- **Wrap your key fob in foil:** This one is tricky. First, you'll have to convince your friends that you haven't fallen for some wacky conspiracy

Card Not Present Fraud , Fraud Management & Cybercrime

Criminals 'Ghost Tap' NFC for Payment Cash-Out Attacks

BANK INFO SECURITY

Tactic Uses Stolen Cards Added to Apple Pay and Google Pay Digital Wallets

Mathew J. Schwartz (euroinfosec) • November 20, 2024

Digital Security

To tap or not to tap: Are NFC payments safer?

Contactless payments are quickly becoming ubiquitous – but are they more secure than traditional payment methods?

Márk Szabó

TECHNOLOGY

One Tech Tip: Protecting your car from the growing risk of keyless vehicle thefts

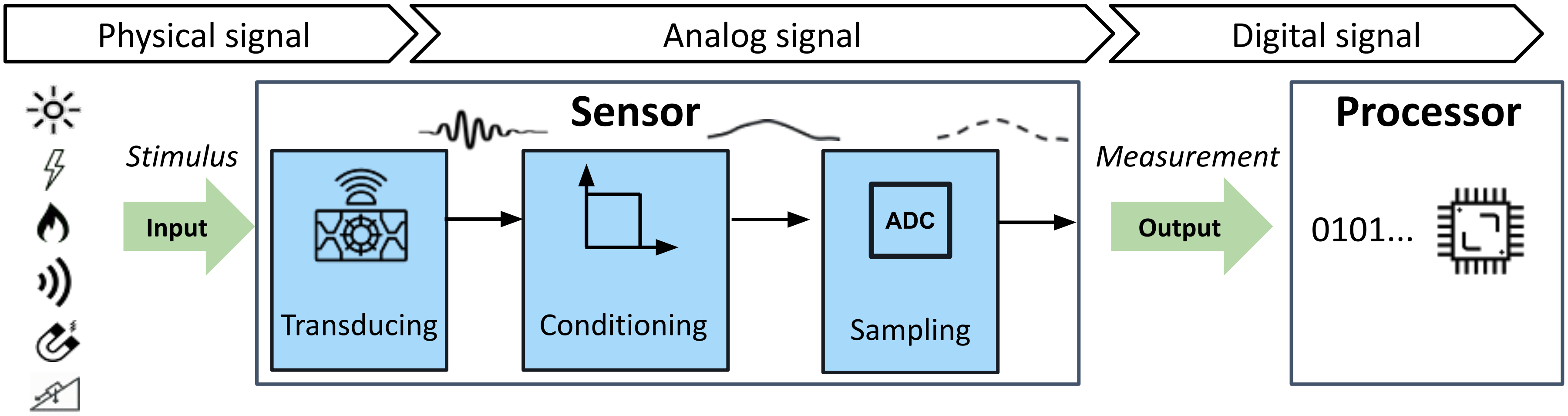
AP

Timeline

Sensing/Actuation

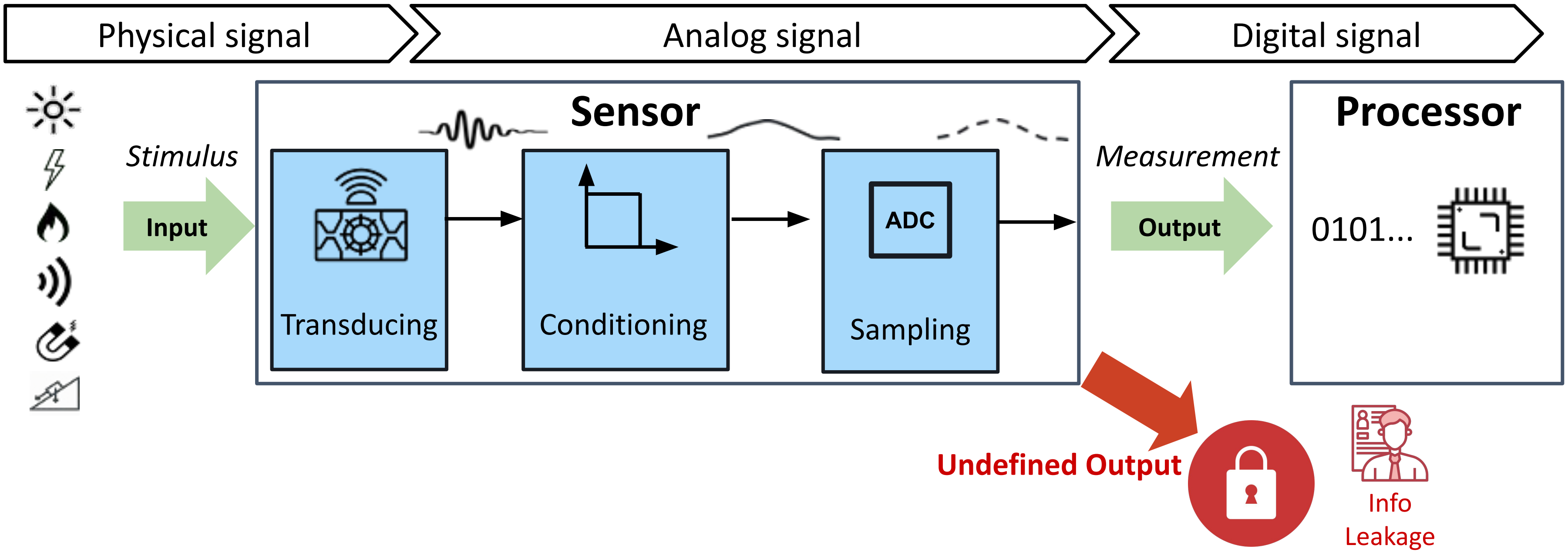
1960s	1980s	2000s	2010s	Today	Future
Embedded Systems (MCUs)	Internet	Embedded Security	IoT Security Medical devices	Home automation Auto. driving AR/VR	AI sys BCI Quant. comp.

Sensing

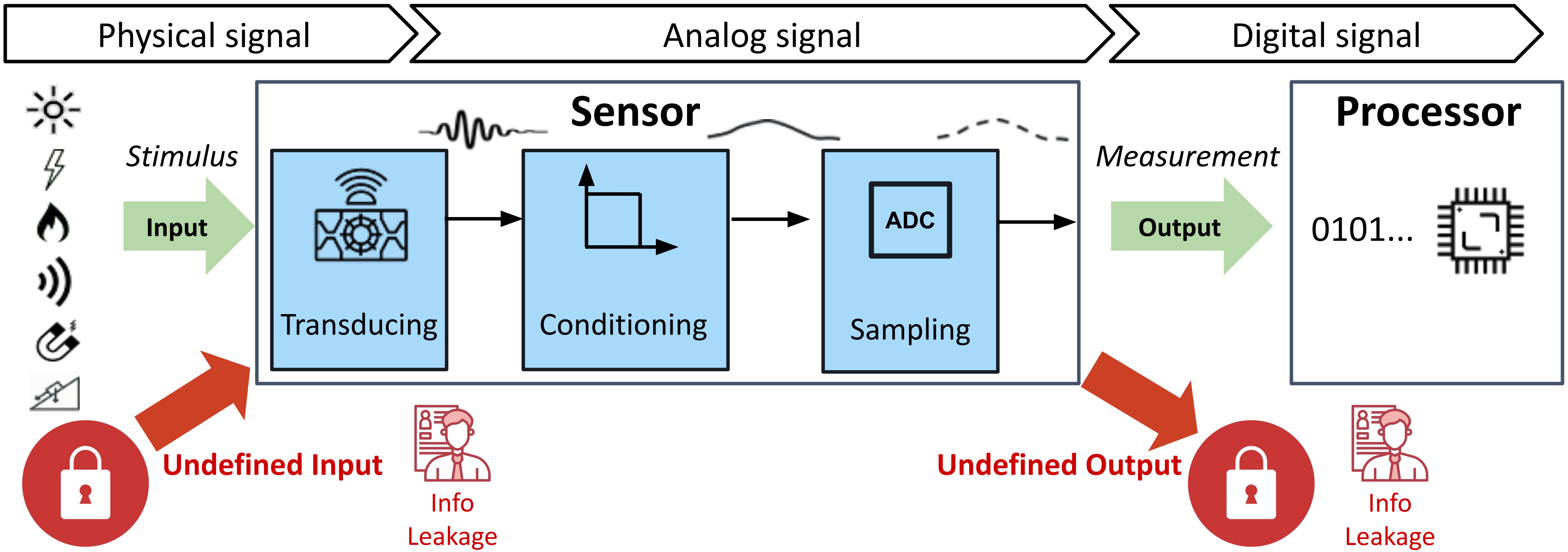


Physical signal
Analog signal
Digital signal
Stimulus
Input
Sensor
Transducing
Conditioning
ADC
Sampling
Measurement
Output
Processor
0101...

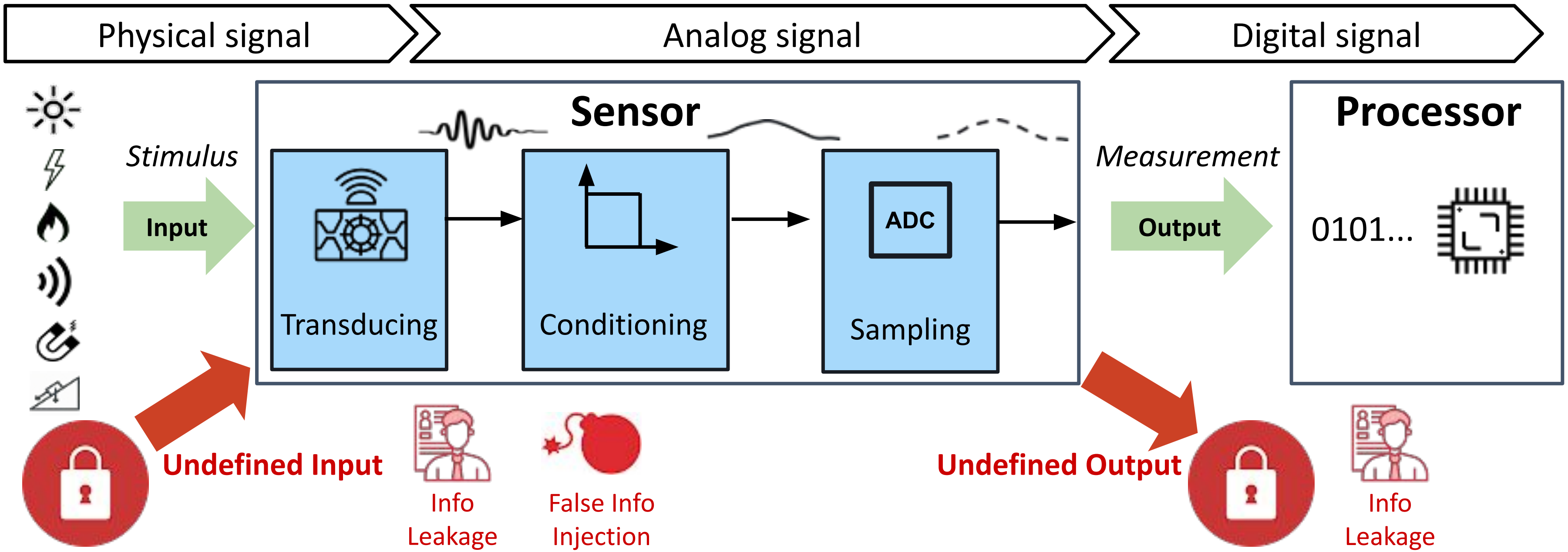
Problem


Physical signal
Analog signal
Digital signal
Stimulus
Input
Sensor
Transducing
Conditioning
ADC
Sampling
Measurement
Output
Processor
0101...
Undefined Output
Info
Leakage

Problem

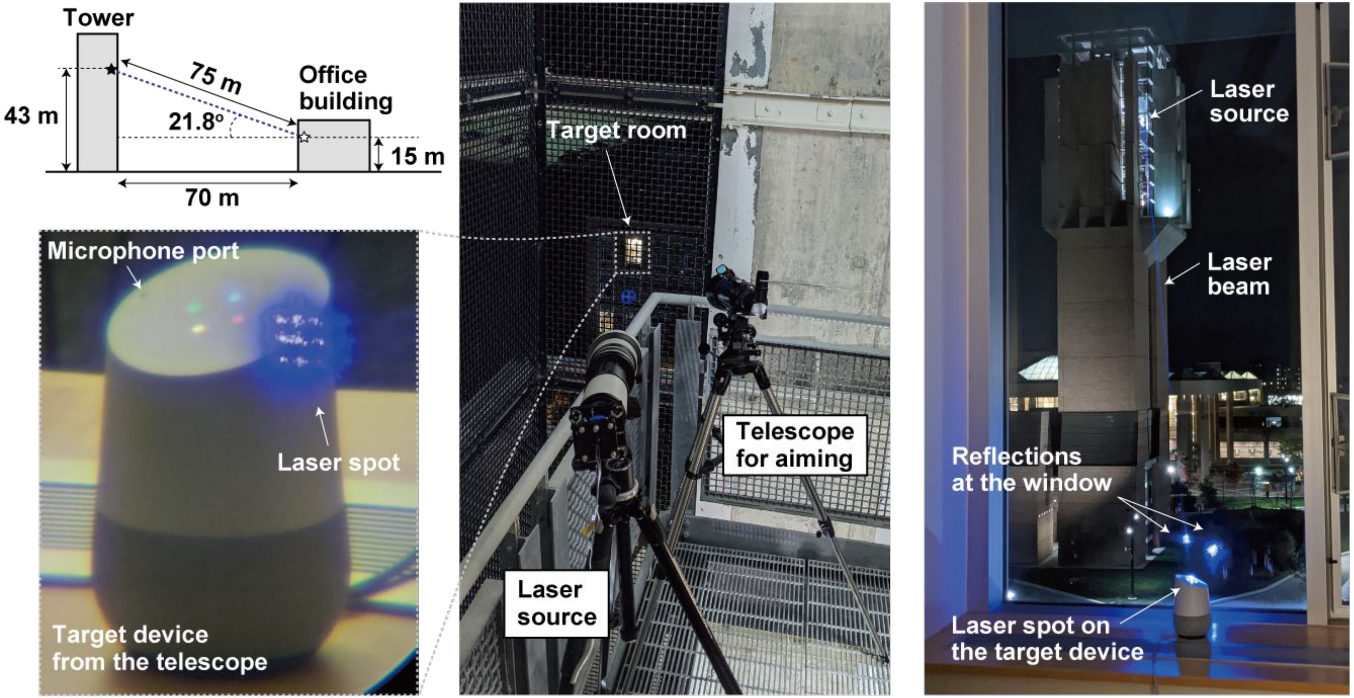

Physical signal
Analog signal
Digital signal
Stimulus
Input
Sensor
Transducing
Conditioning
ADC
Sampling
Measurement
Output
Processor
0101…
Undefined Input
Info
Leakage
Undefined Output
Info
Leakage

Problem



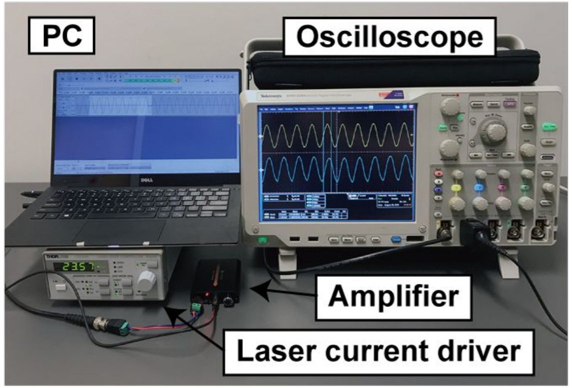
Physical signal
Analog signal
Digital signal
Sensor
Processor
Stimulus
Input
Transducing
Conditioning
ADC
Sampling
Measurement
Output
0101...
Undefined Input
Info Leakage
False Info Injection
Undefined Output
Info Leakage

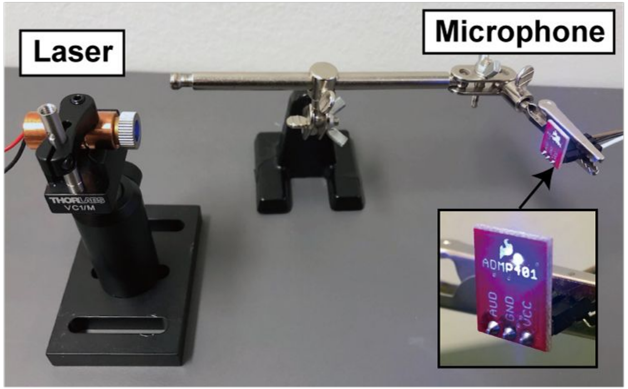
Laser Injection into Microphones

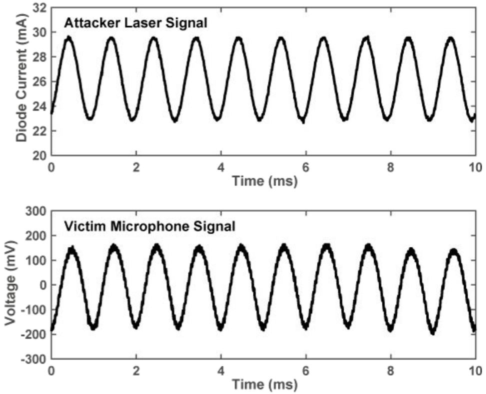


[“Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems ”, Sugawara et al., USENIX Security 2020]

Laser Injection into Microphones

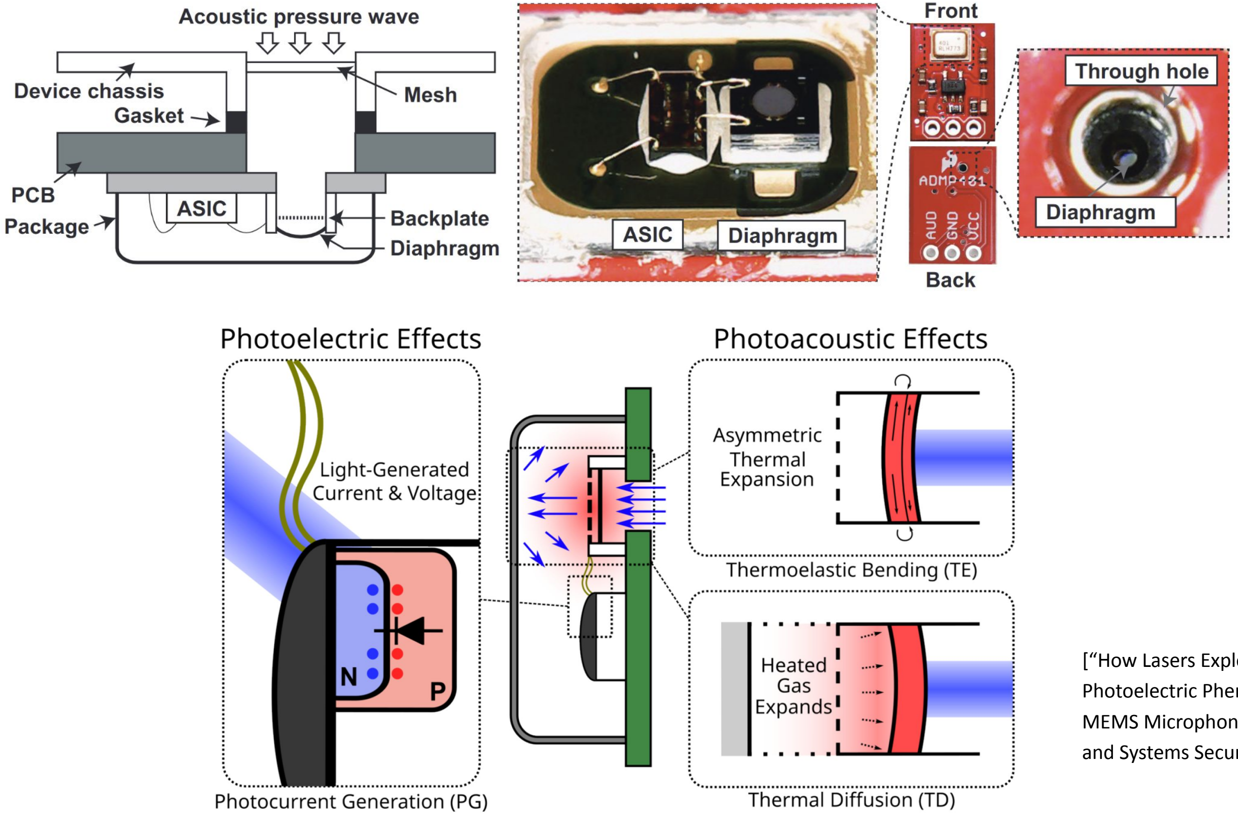






[“Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems”, Sugawara et al., USENIX Security 2020]

Laser Injection into Microphones



[“How Lasers Exploit Photoacoustic and Photoelectric Phenomena to Inject Signals into MEMS Microphones ”, Cyr et al., Journal of Hardware and Systems Security, 2025]

Cameras Capturing Sound?

[AnandTech]

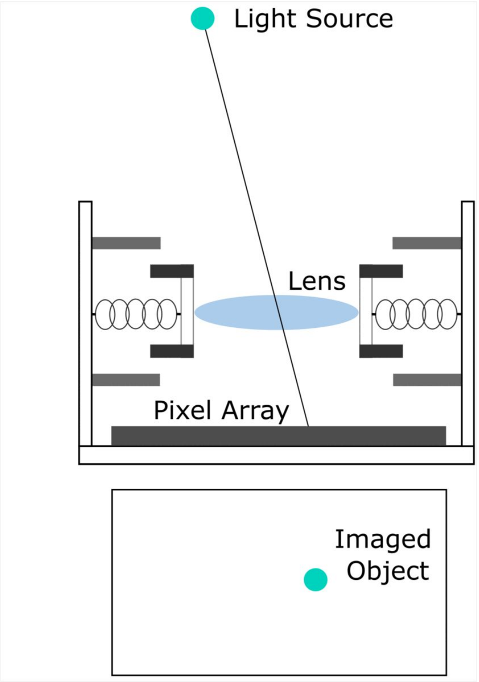
Side Eye

Sound information captured by camera?

Camera

Sensor

Image



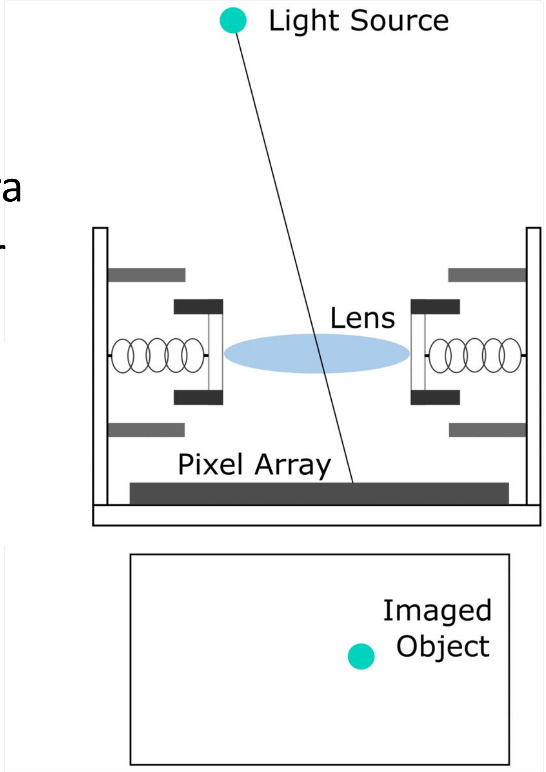
$$f(Sound) = Image$$

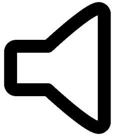
$$g(Image) = \widetilde{Sound}$$

[“Side Eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses ”, Long et al., IEEE SP 2023]

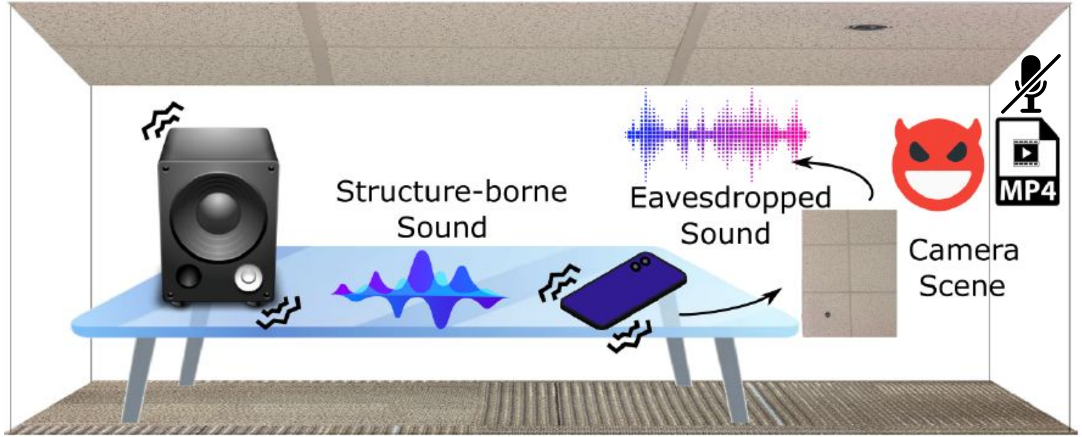
Threat Model

Camera Sensor



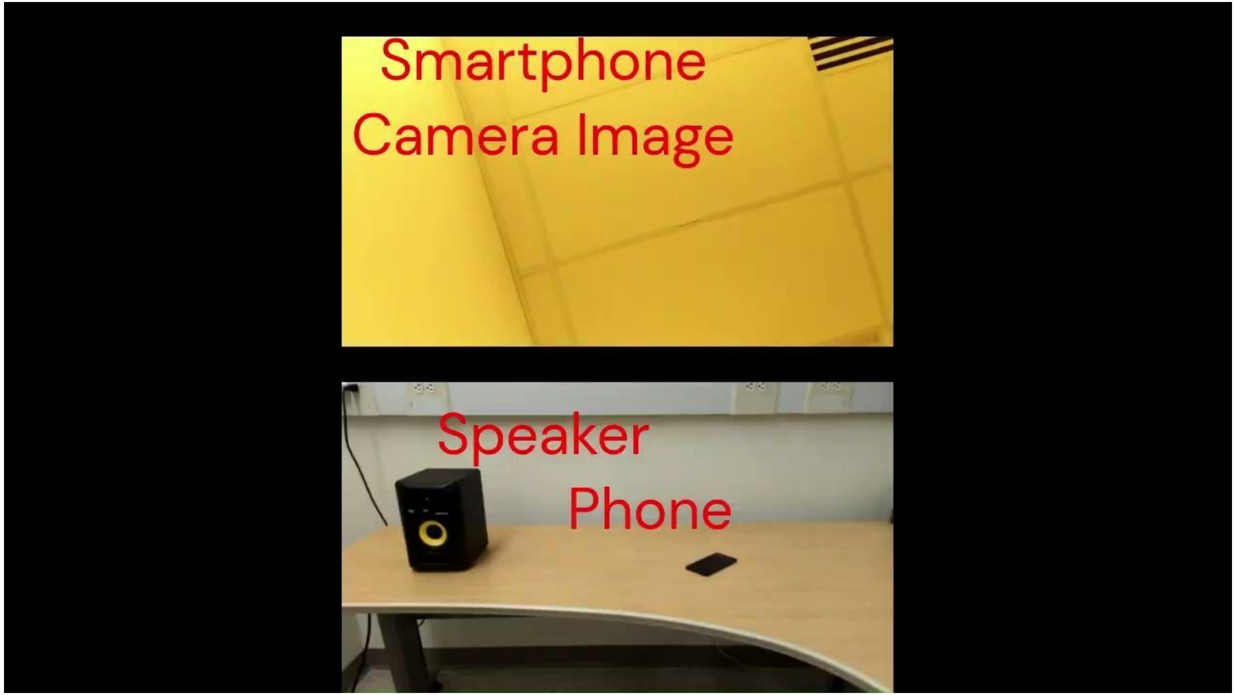


Image



[“Side Eye”, Long et al., IEEE SP 2023]

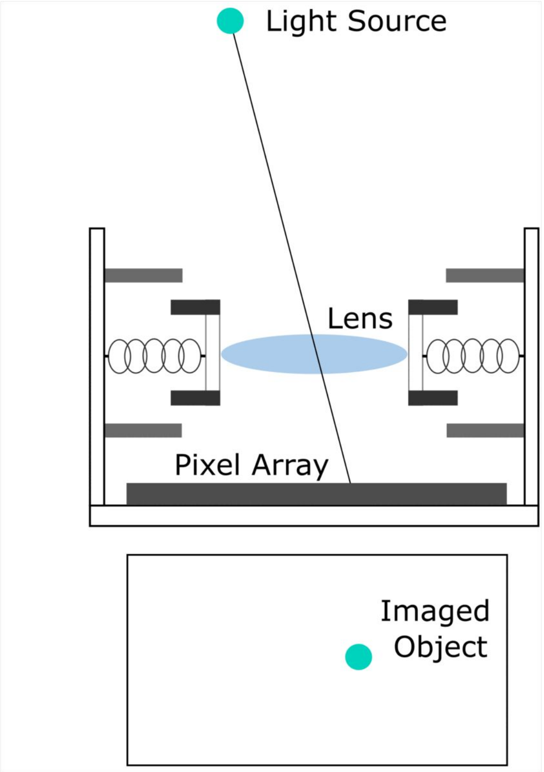
Point-of-view Variations



Audio Samples:
https://sideeyeattack.github.io/Website/

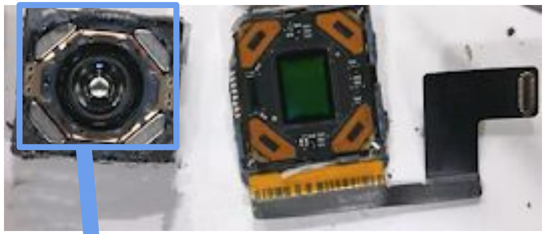
Point-of-view Variations

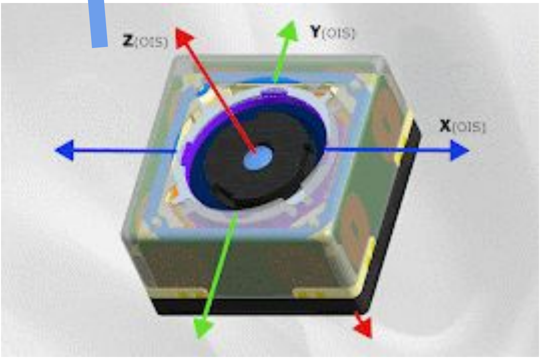
Camera
Sensor



Image

Movable Lens

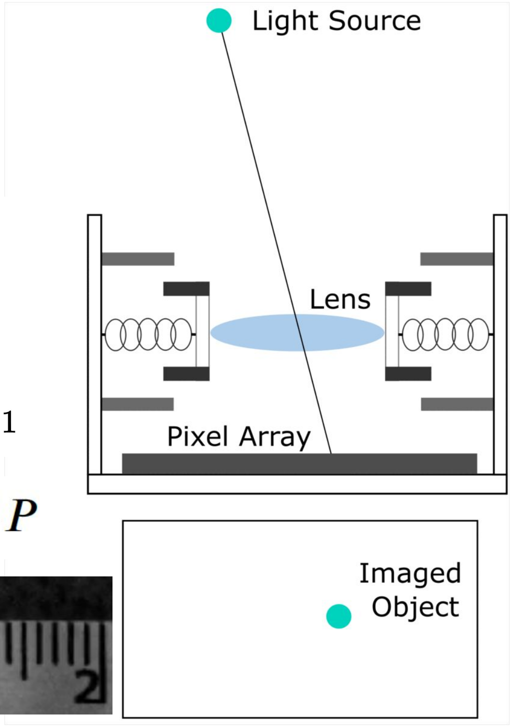




Optical Image Stabilization (OIS)

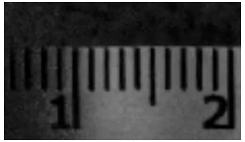
Movable Lens -> Blur Amplification

Camera Movement Dominated

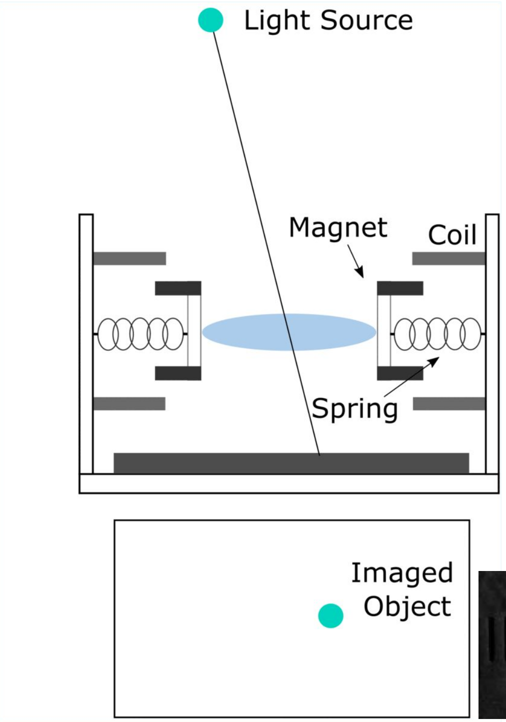


$$\frac{f}{d} \ll 1$$

$$D_{ip} = \frac{f}{d}\frac{A_p}{H}P$$



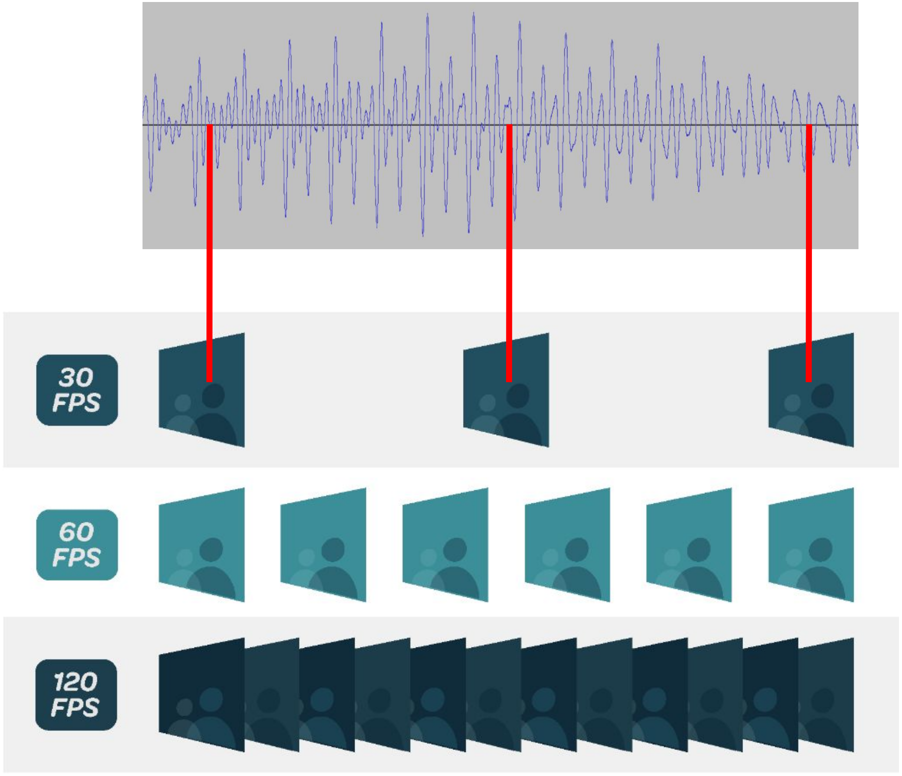
Lens Movement Dominated (OIS)



Signal Amplified

$$D_{il} = (1 + \frac{f}{d})\frac{A_l}{H}P$$

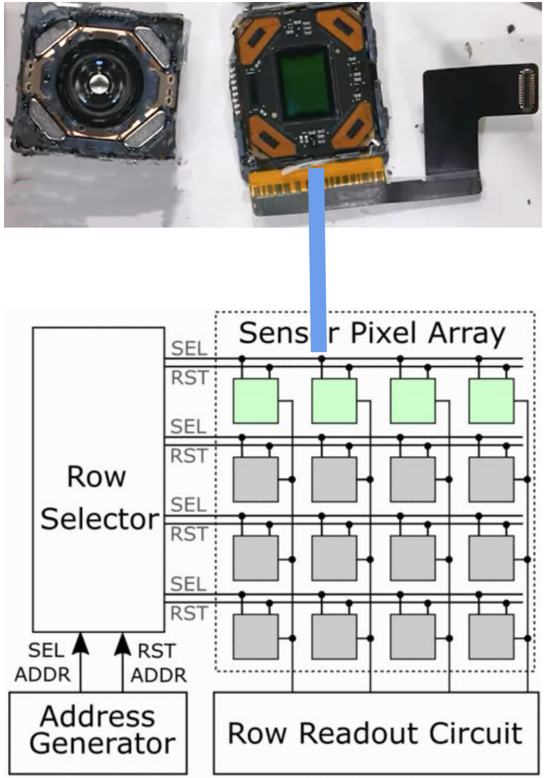
Signal Sampling Rate

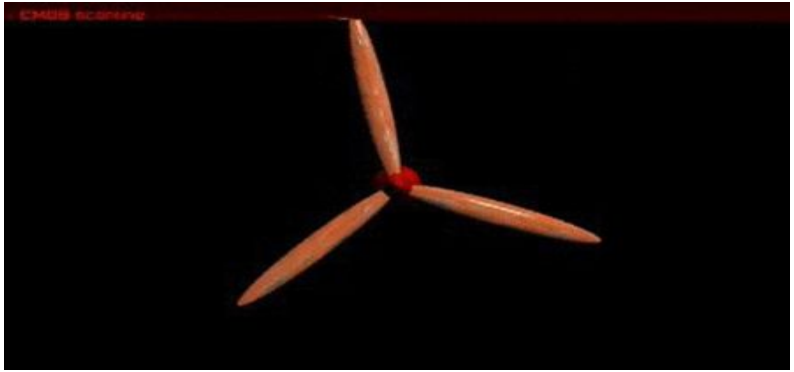


Audio Signal

Limited sample rate/ bandwidth posed by the video frame rate (30-120 Hz)

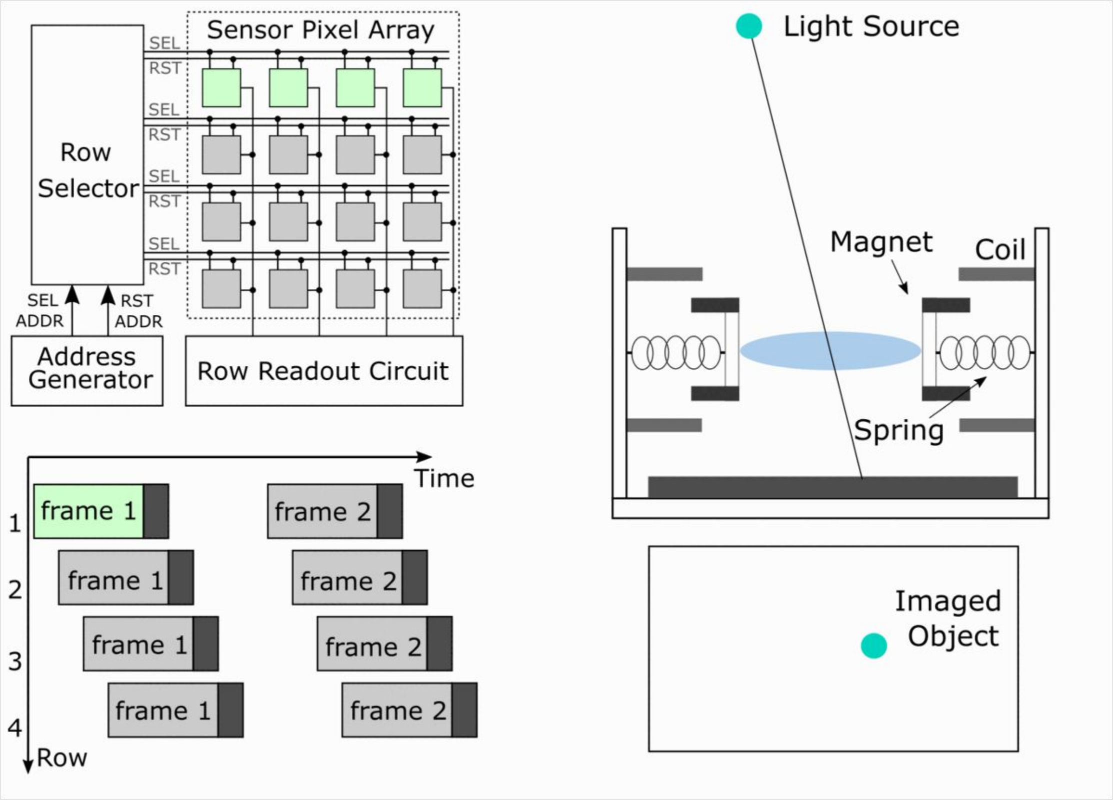
Rolling Shutter



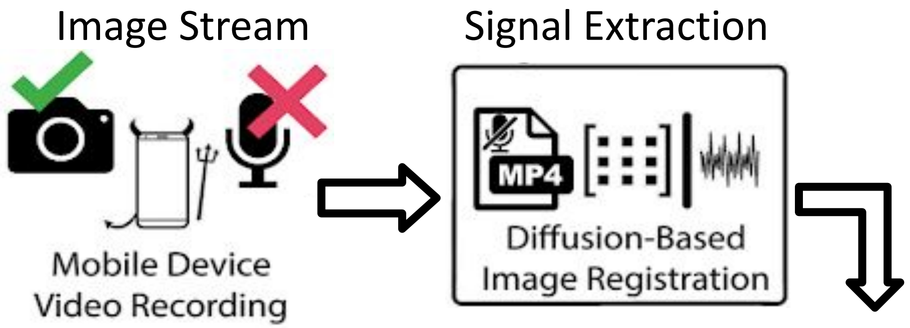


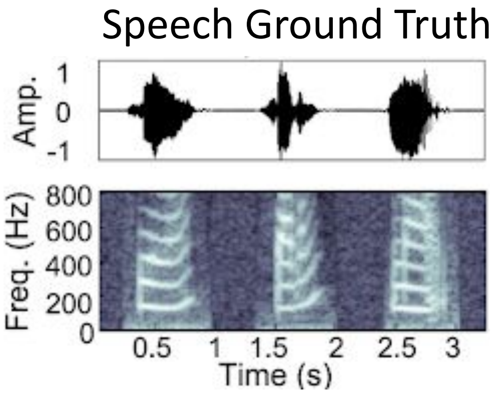
[Photo: David Adler]

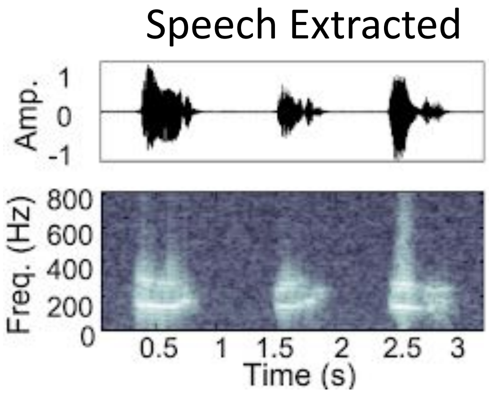
Rolling Shutter -> 1000x Sample Points



Audio Extraction

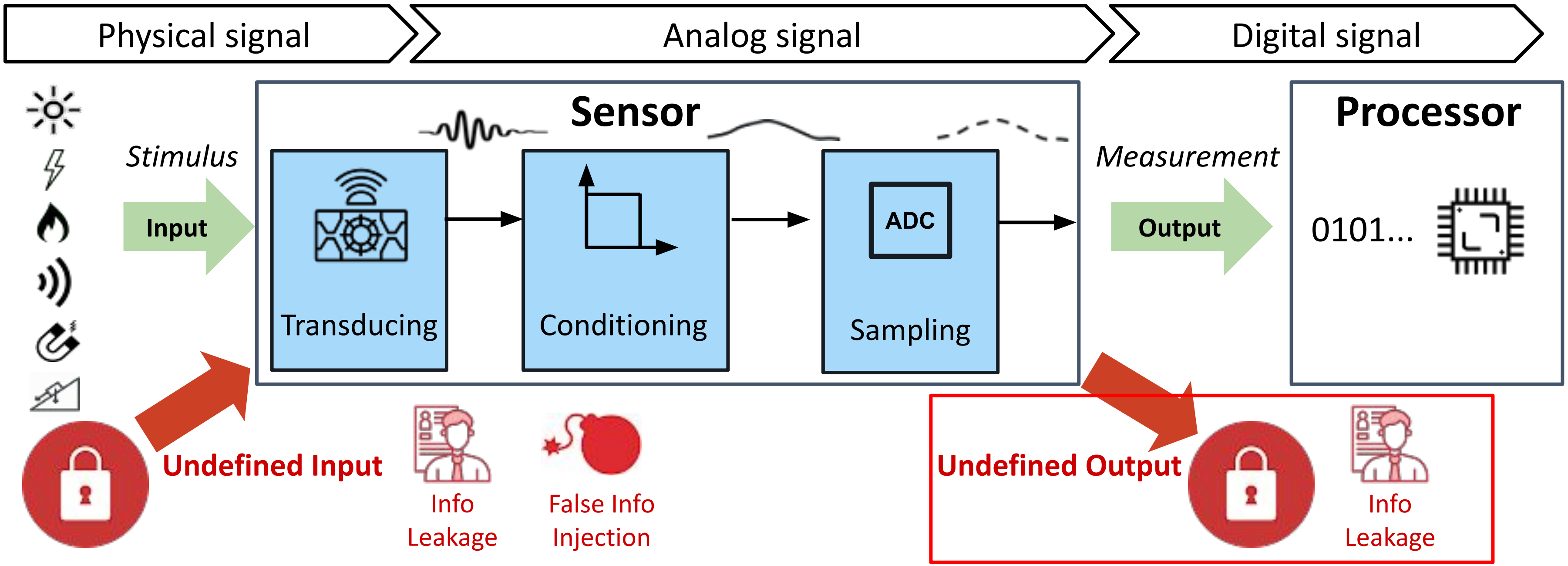






Audio Samples:
https://sideeyeattack.github.io/Website/

Problem



Physical signal
Analog signal
Digital signal
Stimulus
Input
Sensor
Transducing
Conditioning
ADC
Sampling
Measurement
Output
Processor
0101...
Undefined Input
Info Leakage
False Info Injection
Undefined Output
Info Leakage

Leakage Through Camera Hardware?

Software Vulnerabilities

Default Password & Unencrypted Comms [Abdalla et al., 2020]

Brute-force Attacks against 4-digit Passwords [Ling et al., 2017]

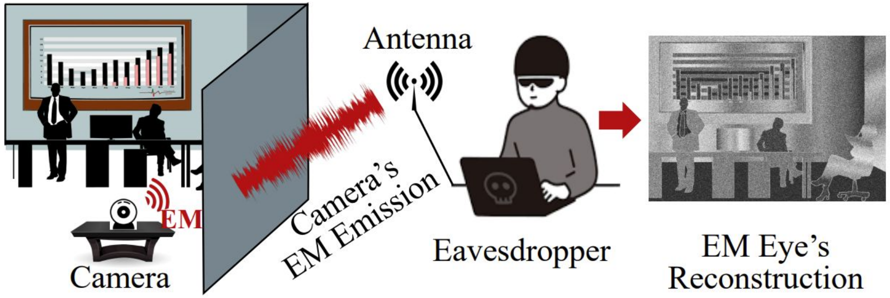
Known Serial Number Camera Hijacking [Herodotou et al., 2023]

Network Traffic Sniffing and Reconstruction [Tekeoglu et al., 2015]

Hardware Vulnerabilities

?

EM Eye

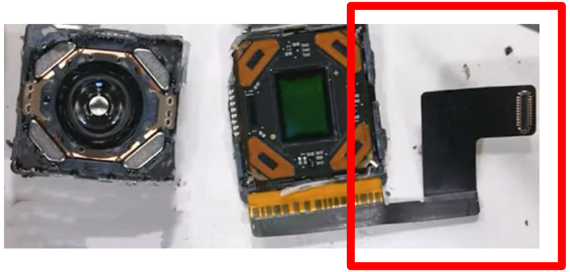


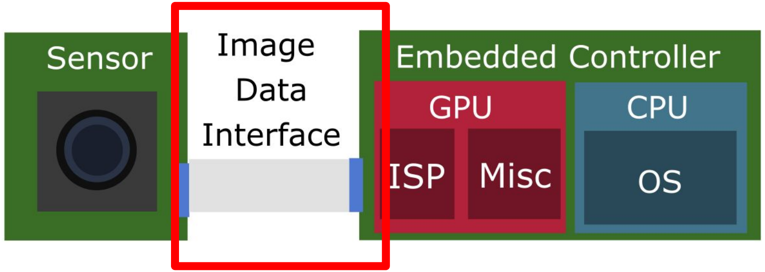
- No software/network entry point
- External physical eavesdropper
- **Unintentional electromagnetic leakage (not wireless comm signals)**

Code, Tutorial, Demo

[“EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras”, Long et al., NDSS 2024]

Embedded Camera Interface





Rambus Products Soluti

Home > Blogs > Automotive > Accelerating MIPI CSI-2 Adoption in Automotive

Back to Blog

Accelerating MIPI CSI-2 Adoption in Automotive

August 15, 2023 by Rambus Press — Leave a Comment

By Joe Rodriguez | Product Marketing Manager, Interface IP

LOW POWER-HIGH PERFORMANCE

MIPI Standards Gaining Traction In New Markets

118 Shares f 47 X 14 in 54

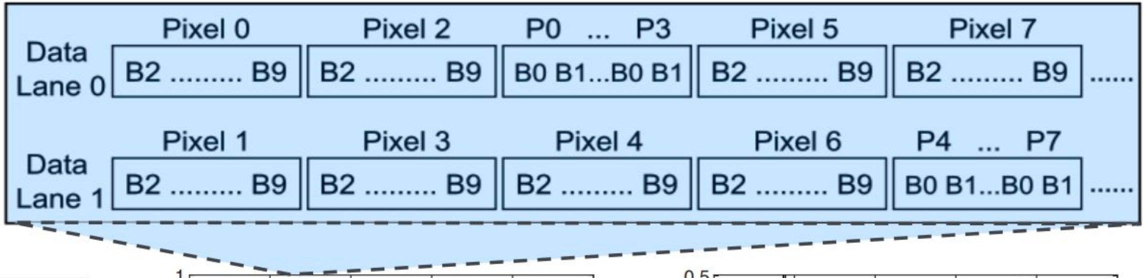
Convergence of vision and AI is driving adoption of MIPI standards beyond just mobile phones.

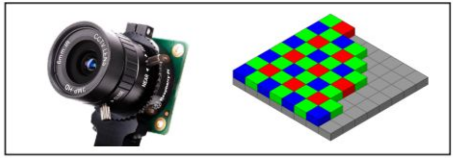
JANUARY 26TH, 2022 - BY: **ANN MUTSCHLER**

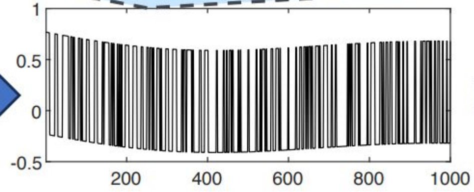
Unprotected Data & EM Emanation

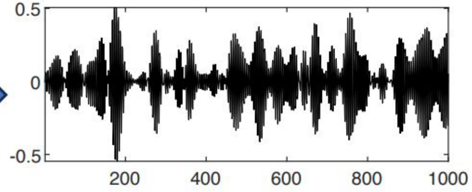
Interface Protocol

Bit Streams of Image Data



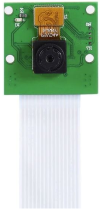




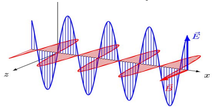


Optic **RAW Digital** **Electromagnetic**

Unintentional Sender

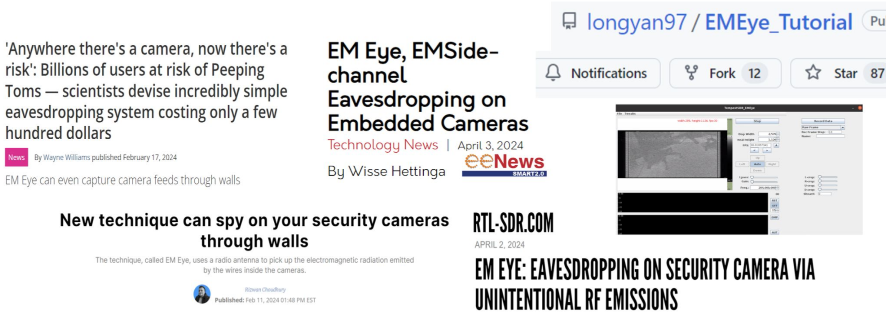


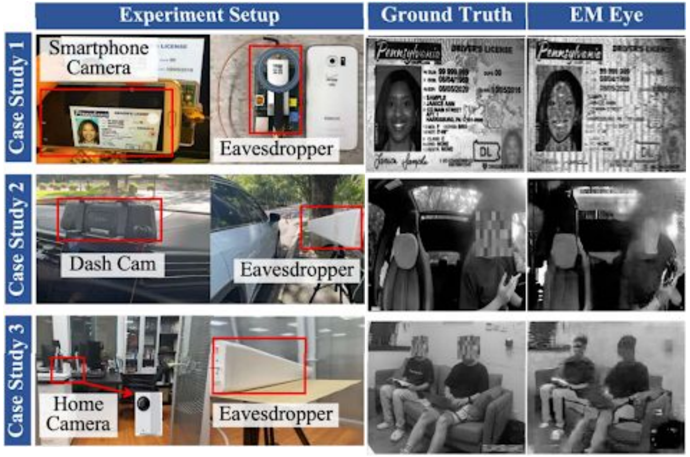
[Maxwell's Equations]

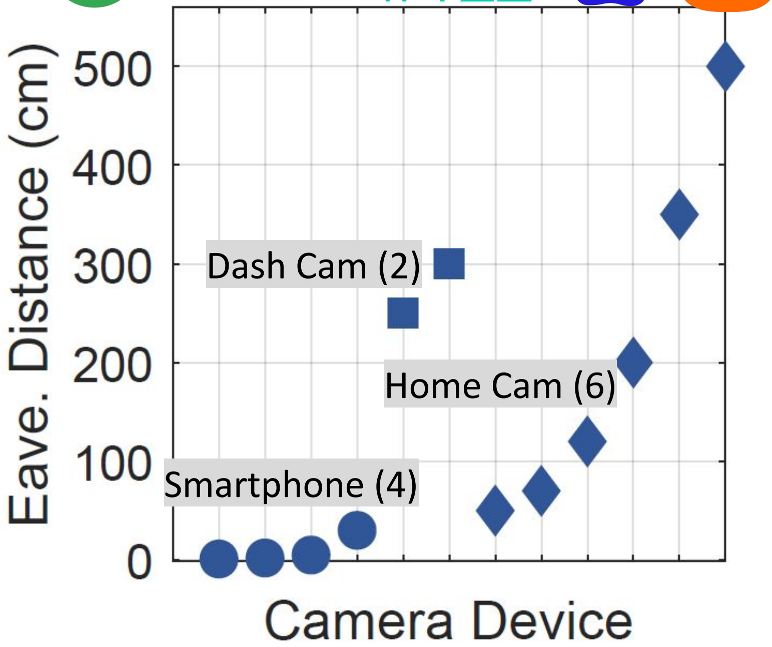


Adversary's Receiver

Affected Devices

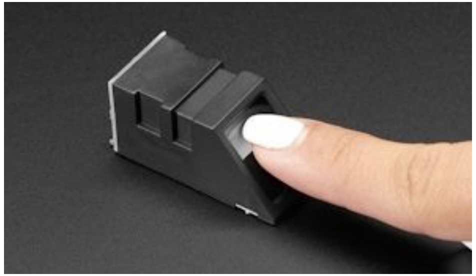






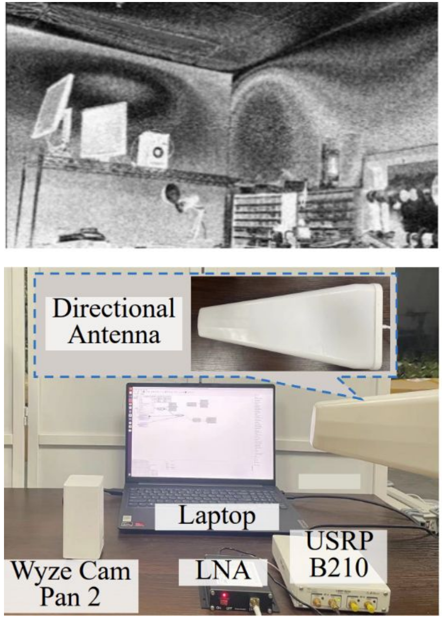
Embedded Data Communication

Other sensors and interfaces: SPI, I2C, ...

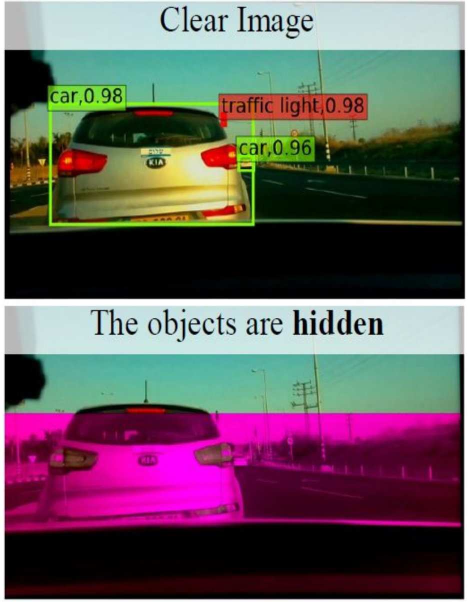


[Photo: Adafruit]

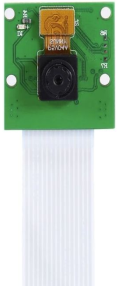
EM Injection Into Cameras



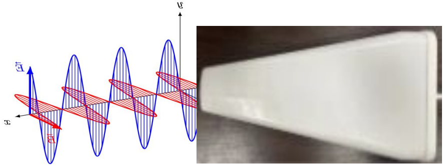
[“EM Eye”, **Long** et al., NDSS 2024]



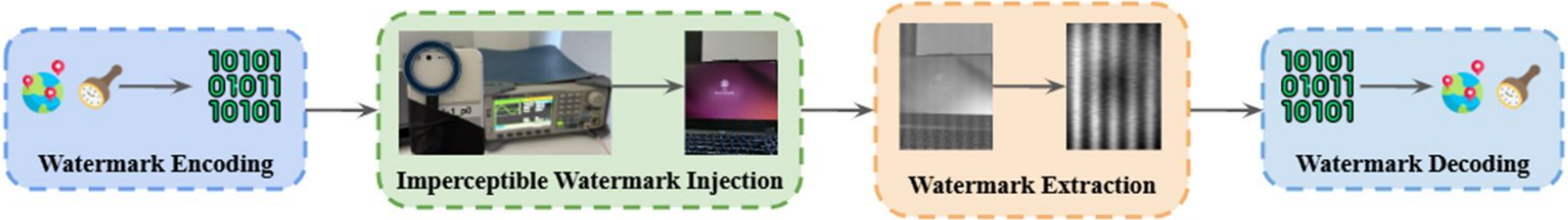
[Jiang et al., USENIX Security 2023]

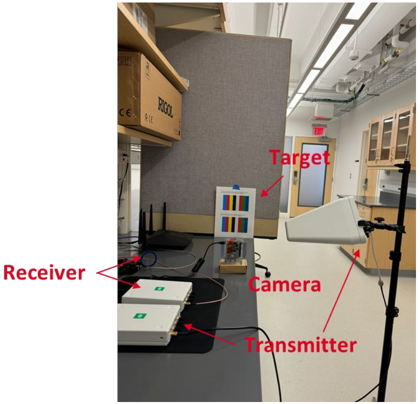


Electromagnetic



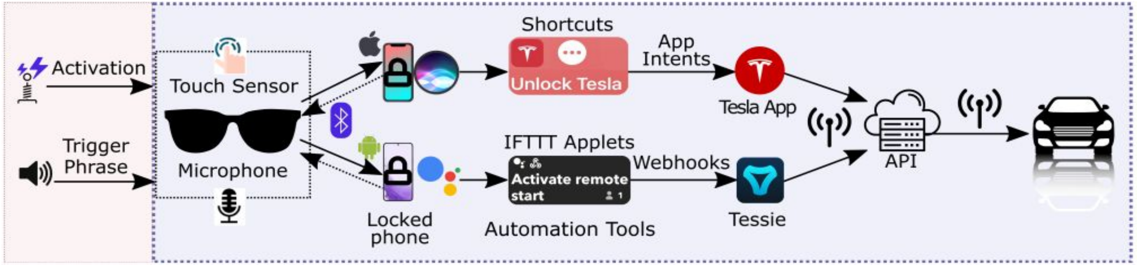
EM Injection Into Cameras: Watermark

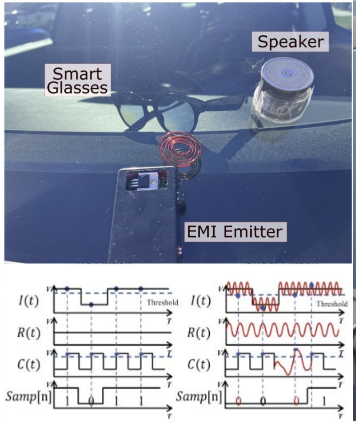


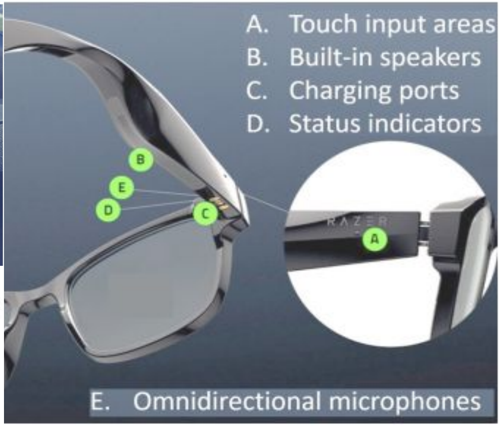


[“RF-Eye-D: Geotagging and Watermarking Camera Imaging Sensors with Radio Frequency Signal Injection”, Ongoing]

Tesla Hijacking in Automated IoT







[“From Virtual Touch to Tesla Command: Unlocking Unauthenticated Control Chains From Smart Glasses for Vehicle Takeover”, Zhang et al., IEEE S&P 2025

Our future…

IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2024, No. 2, pp. 735–768. DOI:10.46586/tches.v2024.i2.735-768

Quantum Circuit Reconstruction from Power Side-Channel Attacks on Quantum Computer Controllers

Ferhat Erata, Chuanqi Xu, Ruzica Piskac and Jakub Szefer

Yale University, New Haven, CT, US
{firstname.lastname}@yale.edu

Feb 2025

1960s	1980s	2000s	2010s	Today	Future
Embedded Systems (MCUs)	Internet	Embedded Security	IoT Security Medical devices	Home automation Auto. driving AR/VR	AI sys BCI Quant. comp.

Our future...

Challenges

- **Analog parts:** data integrity and confidentiality protection
- **Model & database:** automated vulnerability discovery
- **Cross-community co-op:** interdisciplinary expertise

Useful Resources:

- CCC Embedded Security White Paper, 2018
- Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.