UCIrvine | The Henry Samueli School of Engineering

Autonomous and Intelligent
Cyber-Physical Systems Laboratory

Cyber-Physical Vulnerabilities in Autonomous Systems: Facing Hard Realities and Shaping the Road Ahead!

Mohammad Al Faruque, Conexant-Broadcom Endowed Chair Professor
ACM Distinguished Speaker and IEEE CEDA Distinguished Lecturer
Director, Center for Resilient Autonomous Systems
Department of Electrical Engineering and Computer Science,
Department of Computer Science,
Department of Mechanical and Aerospace Engineering,
University of California, Irvine (UCI)

UAV for Autonomous Target Tracking

- Drone can perform autonomous tracking powered by advanced AI models **(Age of Physical AI)**
- Commercial Products (Personal Photography and Vlogging)
- Other usage
  - Law Enforcement, Border Protection, and Disaster Relief
  - Illegal Stalking & Harassment

Surveillance Drones for Law enforcement

Commercial Product: DJI Active Track Demo

Drones for Illegal Stalking

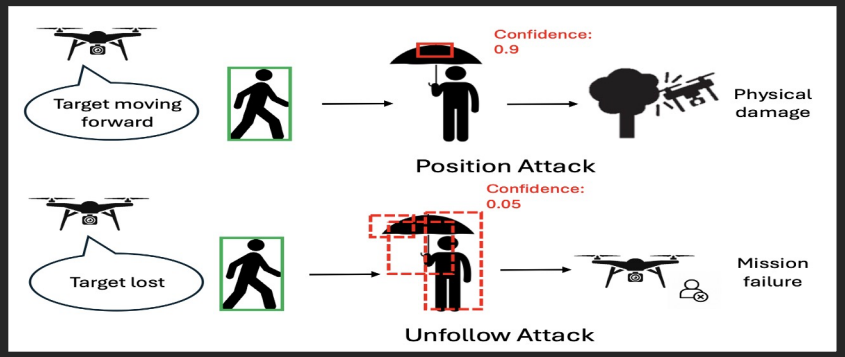
Attacking UAVs for Autonomous Target Tracking

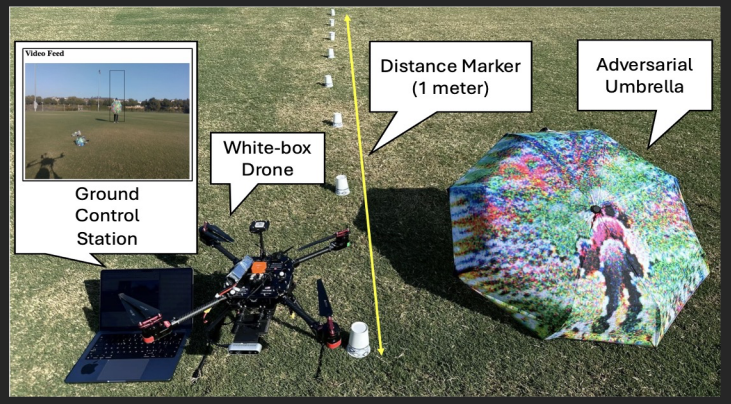
- Physical adversarial attack on UAV systems with ML-based Autonomous Target Tracking (ATT) – Attacking Physical AI
- The attack aims to cause **(i) Drone Crashing** by manipulating its position or **(ii) Mission Failure** by untracking objects
- **Cyber-Exploit**: Physical Adversarial Patches **(Adv. Umbrella)**

Adversarial Model Specifications

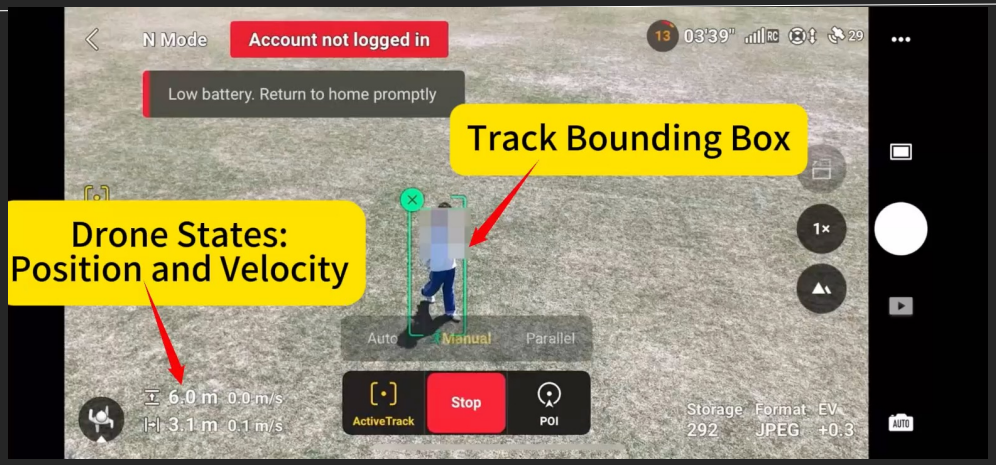
- **Attacker's Motives:**
  - **Good Motive:** Anti-tracking for privacy protection
  - **Bad Motive:** Escape from being tracked (e.g., law enforcement)
- **Attacker's Goals:**
  - **Position Attack:** Manipulate the position of the drone
  - **Unfollow Attack:** Hover and stop tracking

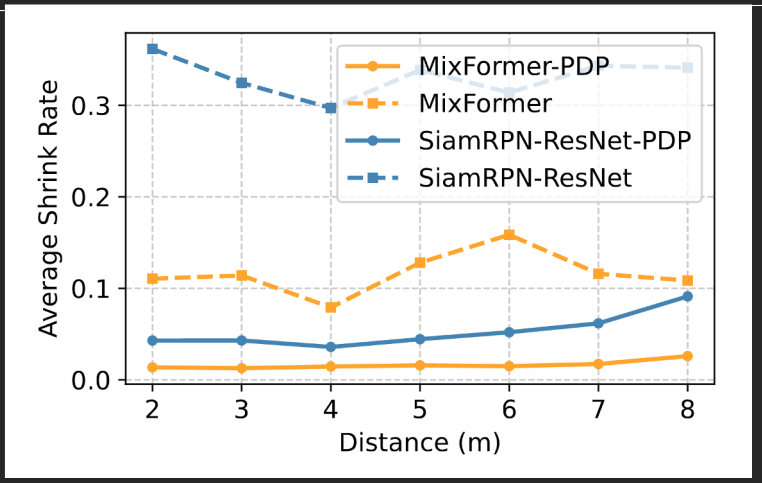
***Position* and *Unfollow* Attacks**





Attack Evaluation





- **Black-box testing** on a commercial drone to verify the distance-pulling vulnerabilities in an autonomous tracking drone
- The attack can successfully pull the drone within the distance of being captured or sensor spoofed
- Analyzed the bounding box shrink rate with the attack distance
  - Progressive distance-pulling (PDP) can work across a wide range of distances, showing physical robustness
  - **Both CNN-based tracker**: **SiamRPN-ResNet** and **Transformer-based tracker**: **MixFormer** are tested

Attack Demonstration

Normal Behaviour
White-box End-to-End system

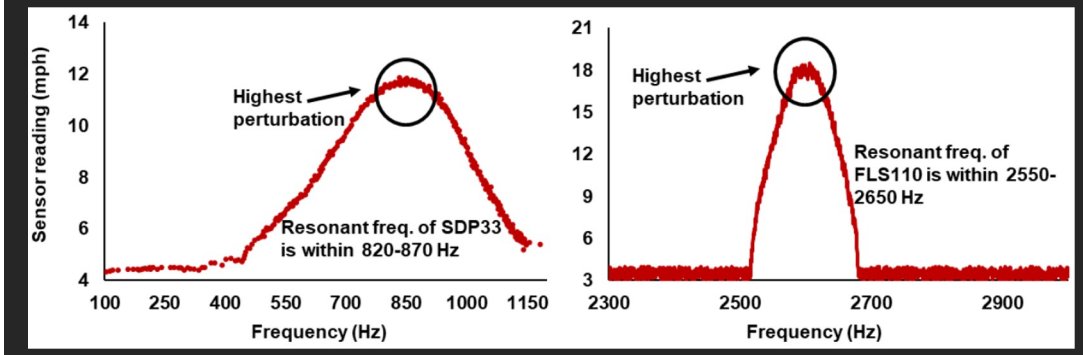
UAV under Attack
White-box End-to-End system

UAV under Attack
Black-box Commercial System

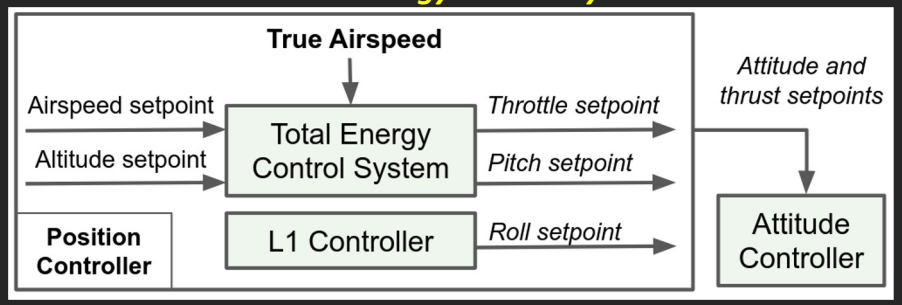
UAV Crash via Airspeed Sensor Spoofing

- Airspeed sensing is crucial for UAV flight dynamics, particularly for regulating throttle, pitch, and overall energy states
- Two key airspeed sensing technologies: differential pressure and hot-wire anemometry → **Both vulnerable to spoofing attacks!!**
- **Cyber-Exploit**: Malicious Acoustic Signals

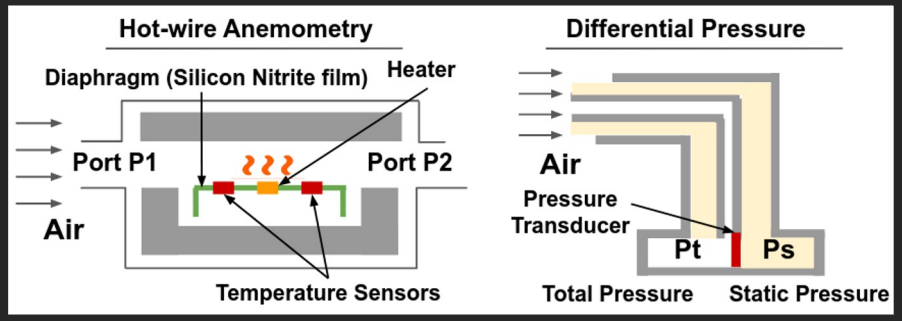
Resonance under acoustic spoofing



UAV Total Energy Control System



Airspeed Sensing Technologies



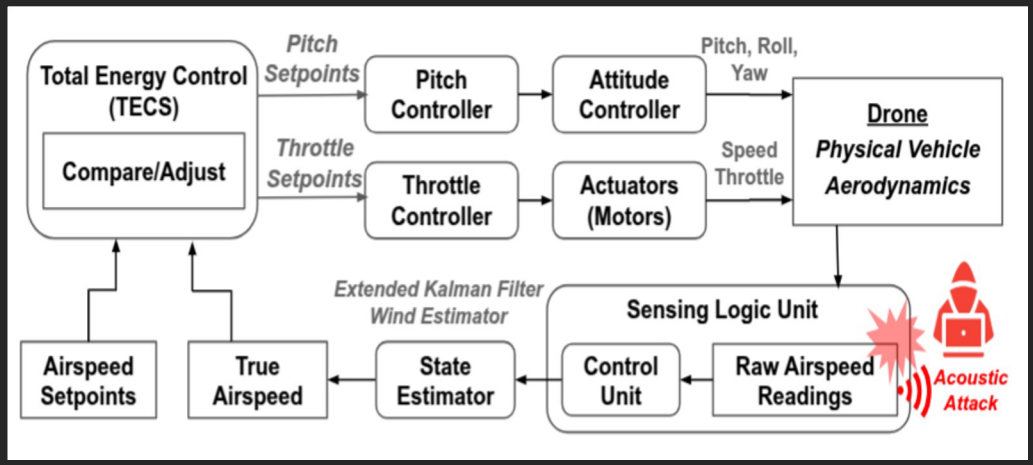
UAV Crash via Airspeed Sensor Spoofing

- **Rationale:** Crash the drone by manipulating throttle and pitch commands via airspeed sensor readings spoofing.
- **Entry Point:** Use acoustic signals at resonant frequency of the airspeed sensor.
- **Attack Goal:** Reduce throttle response to cause aerodynamic stalls. Introduce faults to pitch commands that lead to cause a loss of altitude.
- **Attack Pre-conditions:**

  (1) Identify sensor characteristics (resonant frequency).

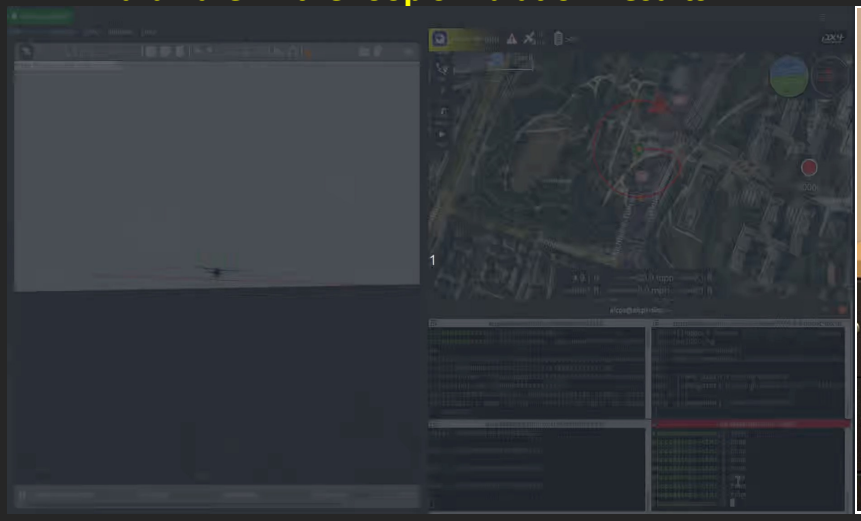
  (2) Powerful audio source within effective range (~few cm)

Overview on the proposed attack model

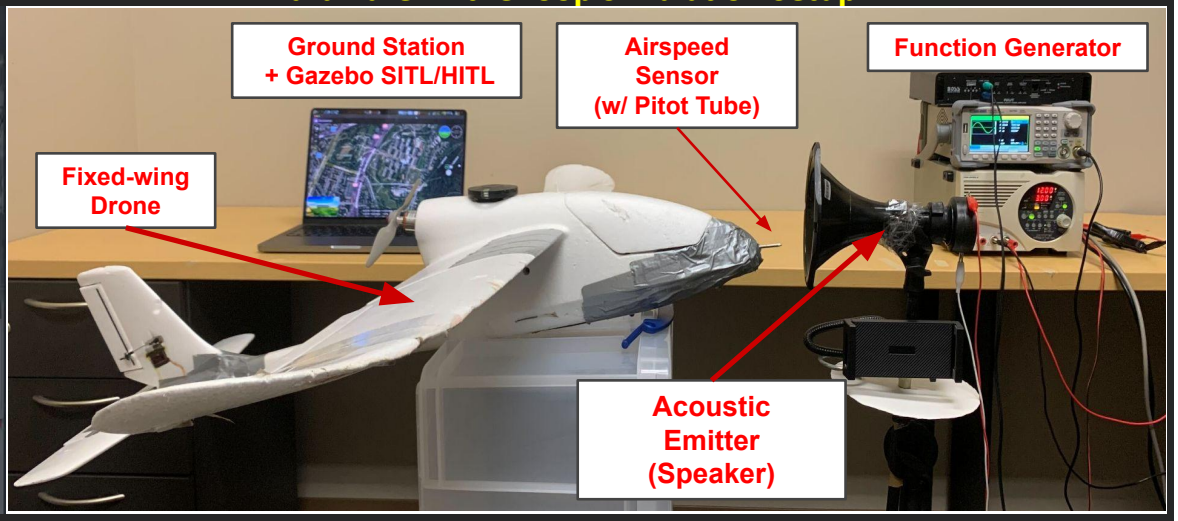


UAV Crash via Airspeed Sensor Spoofing

Hardware-in-the-loop Simulation Results



Hardware-in-the-loop Simulation Setup



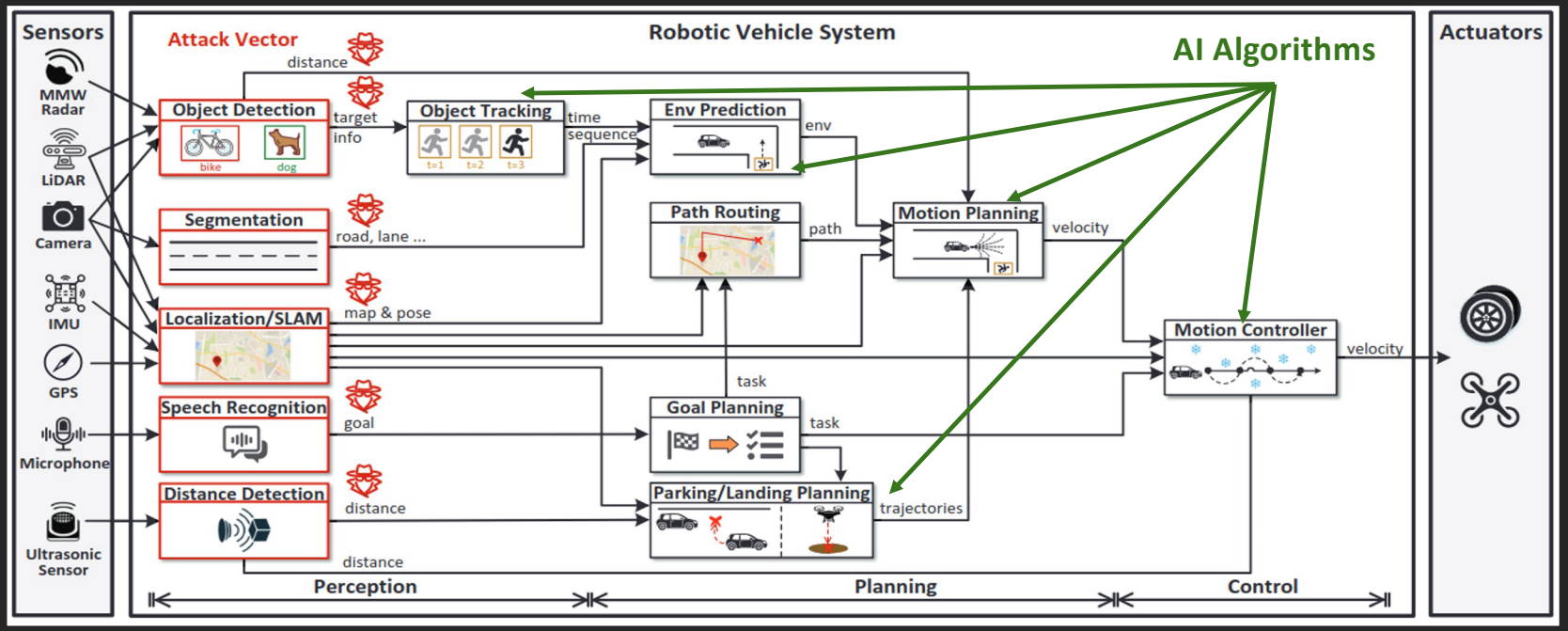
UCI Team Collaborates on $15M Grant to Secure Cyber-Physical Systems

Sept. 3, 2024 - Each week, people in Los Angeles and San Francisco are taking more than 100,000 rides in self-driving vehicles, known as robotaxis. "As autonomous cyber-physical systems, such as autonomous cars, drones, and rovers, are increasingly used in everyday life, the security vulnerabilities of such systems are becoming more exposed to real-world attackers," says Alfred Chen, a professor of computer science at UC Irvine. "This can result in life-critical threats to human safety."

Chen and his team of researchers in the

Next Challenge: From Sensor -to- AI Models

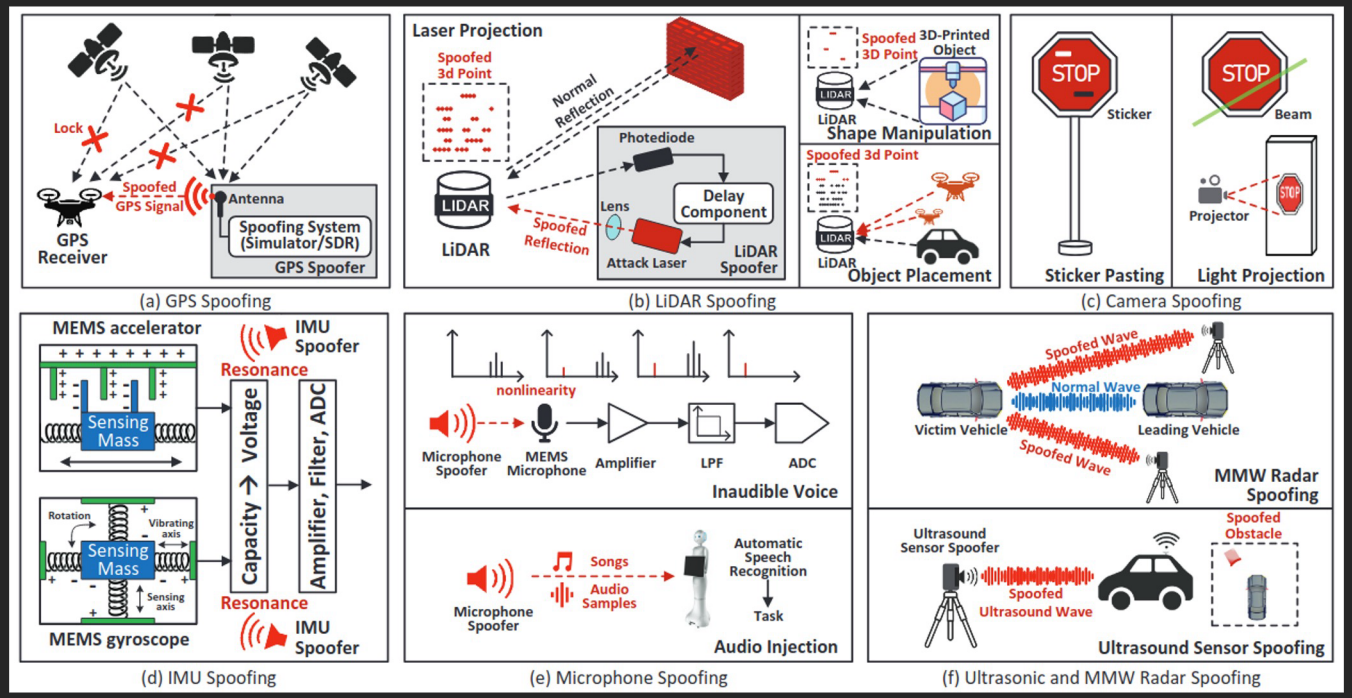
Future RV Systems will be AI-based: How sensor spoofing attacks will impact AI-based RV Systems?



Xu, Yuan, et al. "SoK: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view." *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2023.

Next Challenge: From Sensor -to- AI Models

Future RV Systems will be AI-based: How sensor spoofing attacks will impact AI-based RV Systems?



Xu, Yuan, et al. "SoK: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view." *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2023.

Cross-Layer Security of Embedded and Cyber-Physical Systems

Transition to CPS from ES

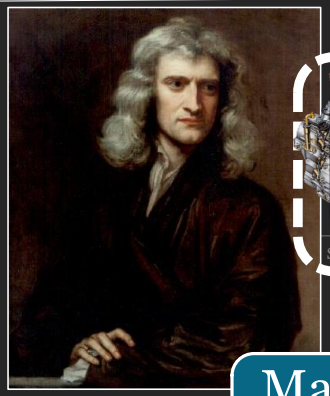
- TU Dortmund Definition: [Peter Marwedel]
  - Embedded systems are information processing systems embedded into a larger product.

- Berkeley: [Edward A. Lee]:
  - Embedded software is software integrated with physical processes. The technical problem is managing time and concurrency in computational systems.

- Cyber-Physical Systems (CPS) are integrations of computation with physical processes [Edward Lee, 2006].
  - The technical problem is managing dynamics, time, and concurrency in networked computational + physical systems.

CPS = Embedded System (ES) + physical Environment

Cyber-Physical System



Physical System

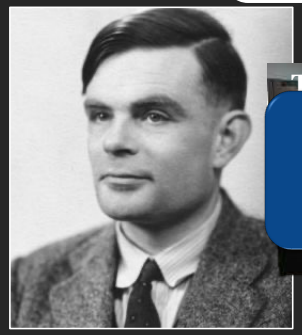
Energy Flow!

Source: http://www.autorepairindy.com/

Observable

Manifested Physically

Sensing



Turing Machine

Information Flow!

Source: http://swizec.com/

Cyber System

Examples of CPS Security

Death toll from Hezbollah pager explosions in Lebanon rises to 12

8 days ago

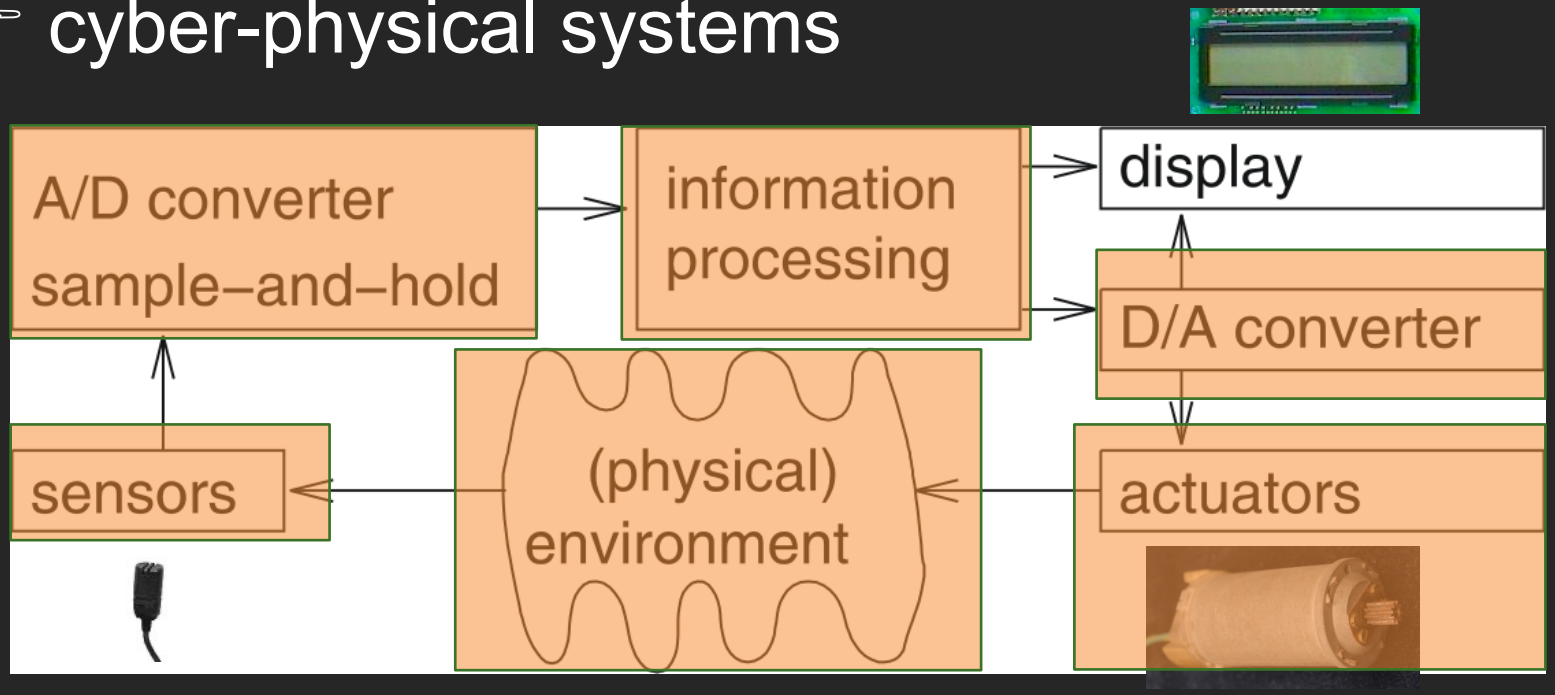
David Gritten
BBC News

Walkie-talkie blasts: attacks on Hezbollah kill 20 as Israel says military focus shifting north

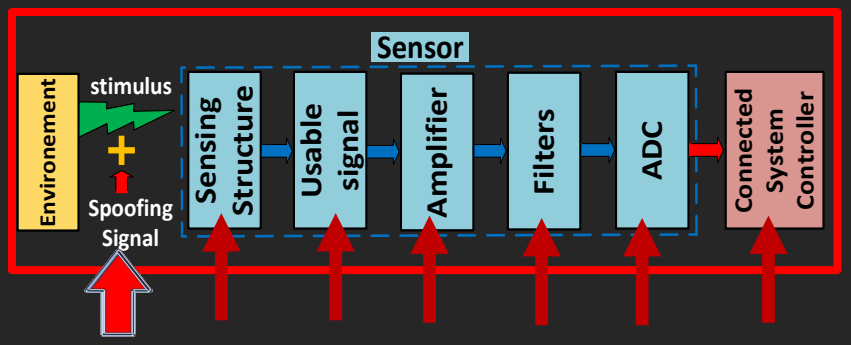
Twenty killed and at least 450 injured in cities across Lebanon a day after exploding pagers killed 12

Abstract View of an Embedded Systems/CPS/Control System

- cyber-physical systems



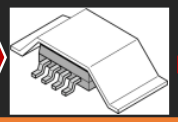
Untrusted Sensor-Hardware



Legitimate input signal, S_{in}

Signal injected by an attacker, S^{f}_{in}

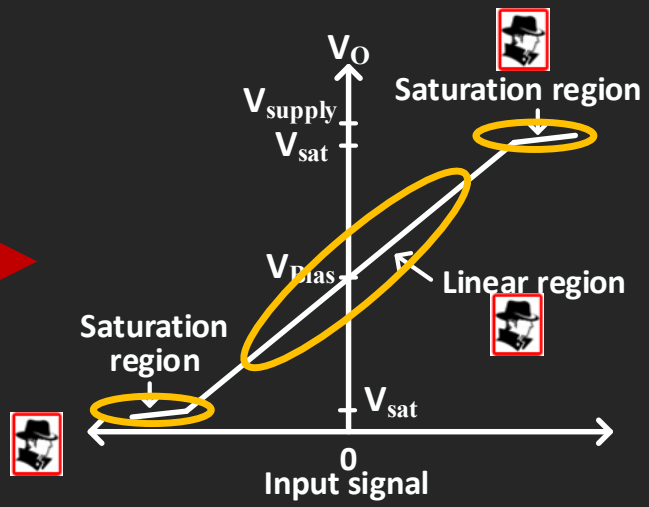
Low-cost external fake stimulus



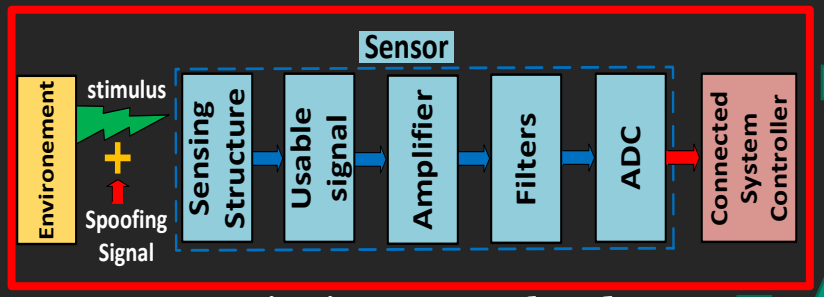
Target Sensor

Spoof in the linear region, drive to the saturation region

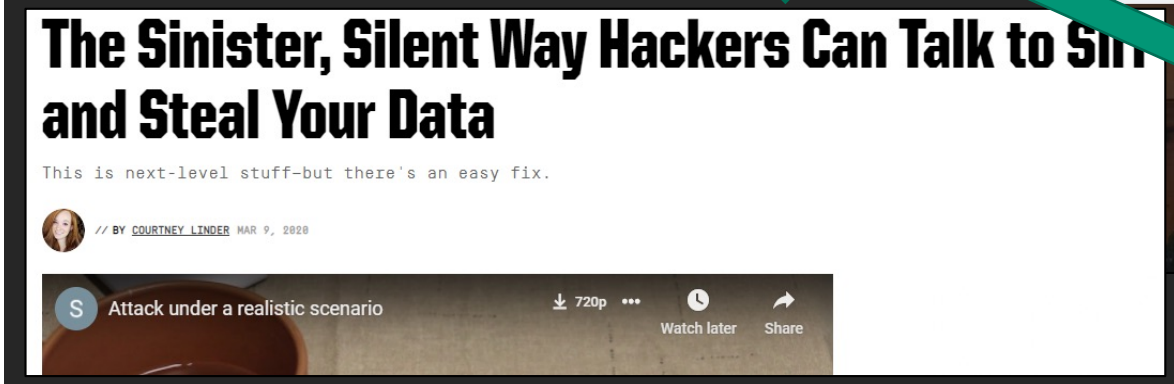
No Security in Sensor- hardware

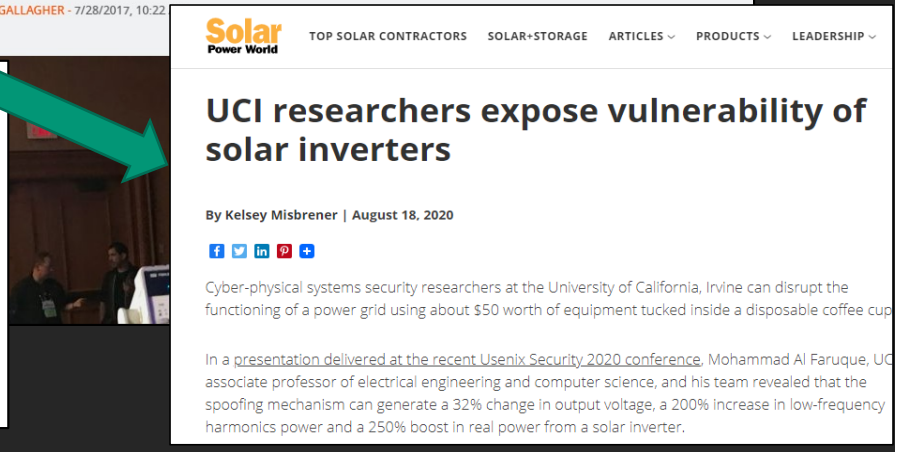


Sensor Spoofing - Compromise Integrity & Availability

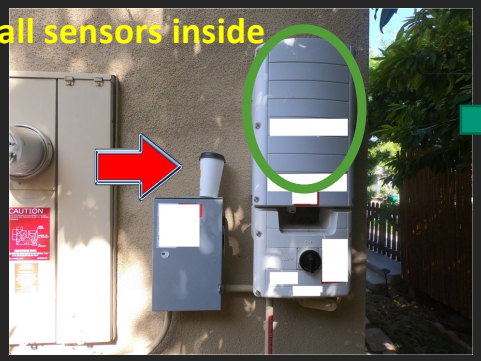


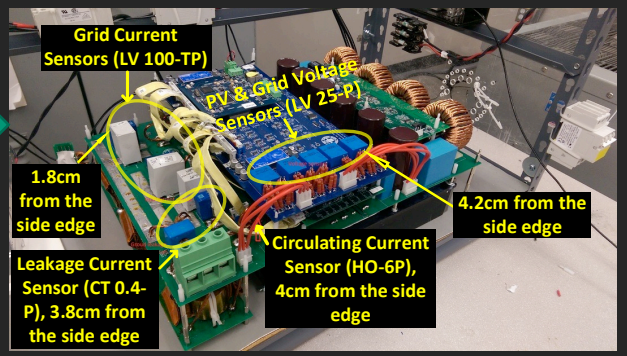
No Security in Sensor- hardware

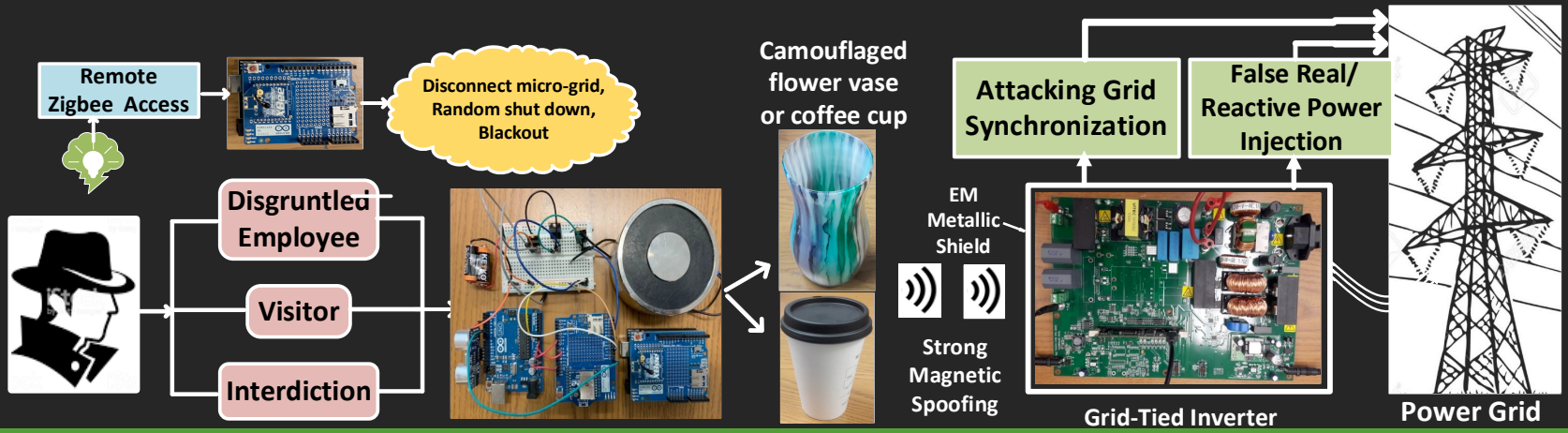




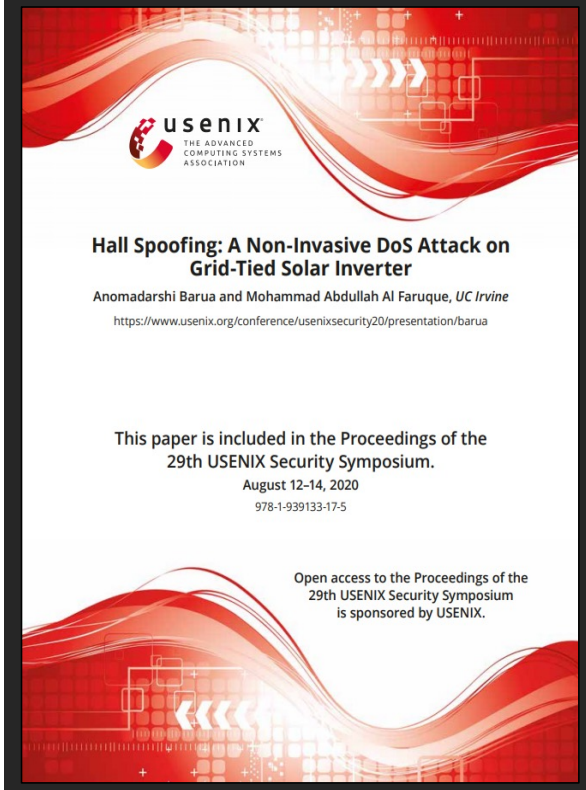
Attack Example 1: Hall Sensors in Grid-Tied Inverters







Our Publication



usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter

Anomadarshi Barua and Mohammad Abdullah Al Faruque, *UC Irvine*

https://www.usenix.org/conference/usenixsecurity20/presentation/barua

This paper is included in the Proceedings of the 29th USENIX Security Symposium.

August 12–14, 2020

978-1-939133-17-5

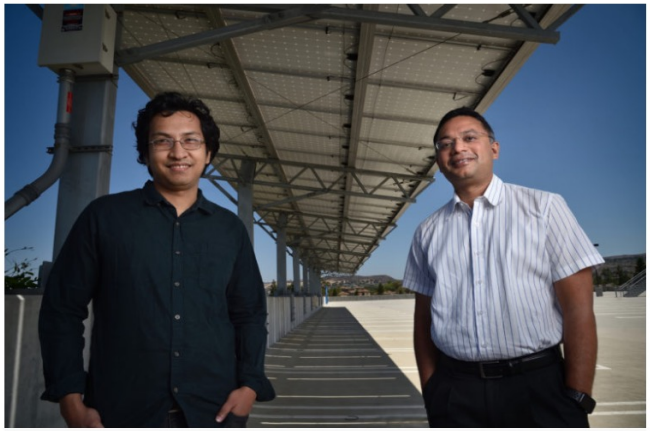
Open access to the Proceedings of the 29th USENIX Security Symposium is sponsored by USENIX.

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

UCI cyber-physical security researchers highlight vulnerability of solar inverters

Device hidden in a coffee cup could destabilize the power grid, triggering a blackout

August 18, 2020



ScienceBlog

Security Researchers Highlight Vulnerability Of Solar Inverters

August 18, 2020 | UC Irvine

Cyber-physical systems security researchers at the University of California, Irvine can disrupt the functioning of a power grid using about $50 worth of equipment tucked inside a disposable coffee cup.

Solar Power World

TOP SOLAR CONTRACTORS | SOLAR+STORAGE | ARTICLES | PRODUCTS | LEADERSHIP

UCI researchers expose vulnerability of solar inverters

By Kelsey Misbrener | August 18, 2020

Cyber-physical systems security researchers at the University of California, Irvine can disrupt the functioning of a power grid using about $50 worth of equipment tucked inside a disposable coffee cup.

In a presentation delivered at the recent Usenix Security 2020 conference, Mohammad Al Faruque, UC associate professor of electrical engineering and computer science, and his team revealed that the spoofing mechanism can generate a 32% change in output voltage, a 200% increase in low-frequency harmonics power and a 250% boost in real power from a solar inverter.

A Wolf in Sheep's Clothing: Spreading Pathogens

A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music

Anomadarshi Barua*
University of California, Irvine
Irvine, CA, USA
anomadab@uci.edu

Yonatan Gizachew Achamyeleh*
University of California, Irvine
Irvine, CA, USA
yachamye@uci.edu

Mohammad Abdullah Al Faruque
University of California, Irvine
Irvine, CA, USA
alfaruqu@uci.edu

ABSTRACT

A Negative Pressure Room (NPR) is an essential requirement by the Bio-Safety Levels (BSLs) in biolabs or infectious-control hospitals to prevent deadly pathogens from being leaked from the facility. An NPR maintains a negative pressure inside with respect to the outside reference space so that microbes are contained inside of an NPR. Nowadays, differential pressure sensors (DPSs) are utilized by the Building Management Systems (BMSs) to control and monitor the negative pressure in an NPR. This paper demonstrates a non-invasive and stealthy attack on NPRs by spoofing a DPS at its resonant frequency. Our contributions are: (1) We show that DPSs used in NPRs typically have resonant frequencies in the audible range. (2) We use this finding to design malicious music to create resonance in DPSs, resulting in an overshooting in the DPS's normal pressure readings. (3) We show how the resonance in DPSs can fool the BMSs so that the NPR turns its negative pressure to a positive one, causing a potential *leak* of deadly microbes from NPRs. We do experiments on 8 DPSs from 5 different manufacturers to evaluate their resonant frequencies considering the sampling tube length and find resonance in 6 DPSs. We can achieve a 2.5 Pa change in negative pressure from a ~7 cm distance when a sampling tube is not present and from a ~2.5 cm distance for a 1 m sampling tube length. We also introduce an interval-time variation approach for an adversarial control over the negative pressure and show that the *forged* pressure can be varied within 12 - 33 Pa. Our attack is also capable of attacking multiple NPRs simultaneously. Moreover, we demonstrate our attack at a real-world NPR located in an anonymous bioresearch facility, which is FDA approved and follows CDC guidelines. We also provide countermeasures to prevent the attack.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**; *Hardware attacks and countermeasures.*

KEYWORDS

Pressure sensors; Resonance; Negative pressure room; Pathogens

ACM Reference Format:
Anomadarshi Barua, Yonatan Gizachew Achamyeleh, and Mohammad Abdullah Al Faruque. 2022. A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music . In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22), November 7–11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3548606.3560643

*Both authors contributed equally to this research.

CCS '22, November 7–11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9450-5/22/11.
https://doi.org/10.1145/3548606.3560643

1 INTRODUCTION

A Bio-Safety Level (BSL) [68, 74] is a set of strict regulations assigned to a biolab or hospital facility to prevent deadly pathogens from being leaked from the facility. The BSL is ranked from BSL-1 (lowest safety level) to BSL-4 (highest safety level) depending on the microbes that are being contained in a laboratory or hospital setting. The Centers for Disease Control and Prevention (CDC) sets BSLs to exhibit specific controls for the containment of microbes to protect the surrounding environment and community.

BSLs require that the isolation rooms in a biolab or infectious-control hospital maintain negative pressure with respect to the outside hallway [74]. Therefore, the room is known as the Negative Pressure Room (NPR). An NPR ensures that potentially harmful microbes cannot leak from the facility through airflow by maintaining negative pressure inside. Therefore, an NPR is critical in preventing deadly bioaerosols from escaping from the facility.

With rising concerns of bioterrorism, an NPR must maintain a certain *negative pressure* following strict regulations established by the CDC, ASHRAE, or other authorities [53, 67]. The Differential Pressure Sensors (DPSs) are commonly used in NPRs to measure the negative pressure in the facility [65]. The DPSs provide the pressure data to the Heating, Ventilation, and Air Conditioning (HVAC) systems, which *maintains* the negative pressure by controlling the airflow into NPRs [79]. In addition, a Room Pressure Monitoring (RPM) system is also present in NPRs to *monitor* the room pressure [7]. The RPM system also depends on the reading from the DPSs installed in an NPR. Both RPM and HVAC systems are connected with the Building Management Systems (BMSs) for automated control and monitoring of the negative pressure in an NPR.

A DPS has an elastic diaphragm working as a pressure force collector. Therefore, a DPS can be modeled as a second-order dynamic system with a resonant frequency [83]. We demonstrate by thorough experiments that the resonant frequencies of DPSs used in NPRS are typically in the audible range. In addition, we show that the DPS with a sampling tube can be modeled as a Helmholtz resonator, and the resonant frequency of a DPS with a sampling tube still falls within the audible range. This finding is important because an attacker, who has an intention to change the negative

ACM CCS 2022

A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music

https://sites.google.com/view/awolfinsheepsclothing/home

Negative Pressure Room against Bioterrorism

A negative pressure room maintains lower pressure inside with respect to the outside reference space

Air flows from outside to inside so that pathogens are trapped inside

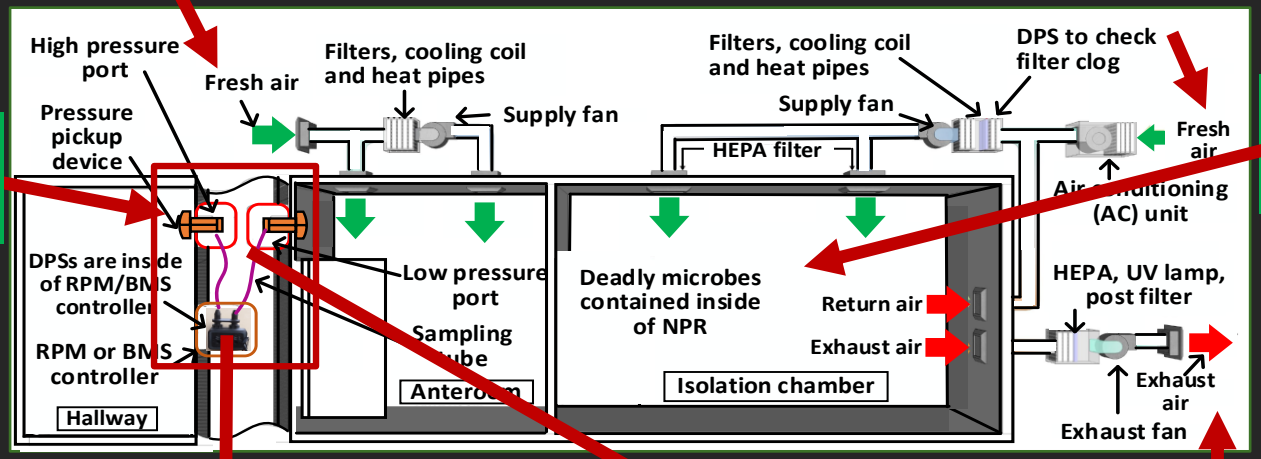
Hospital

Research facilities

Pharmacy

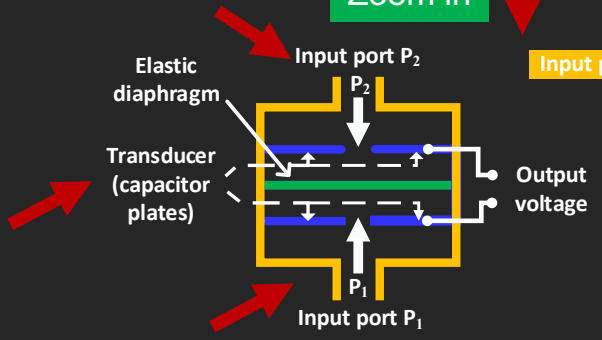
Details of Negative Pressure Room and Pressure Sensor

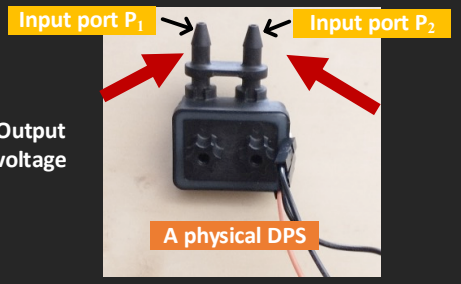
Differential pressure sensor maintains negative pressure

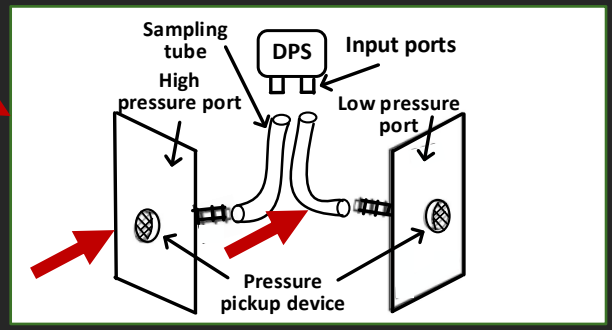


Prevent airborne particles like bacteria and viruses from spreading out

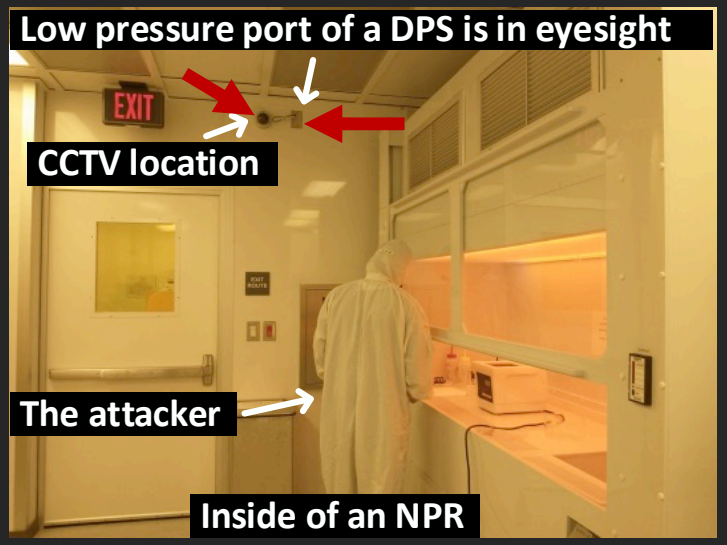
Zoom in

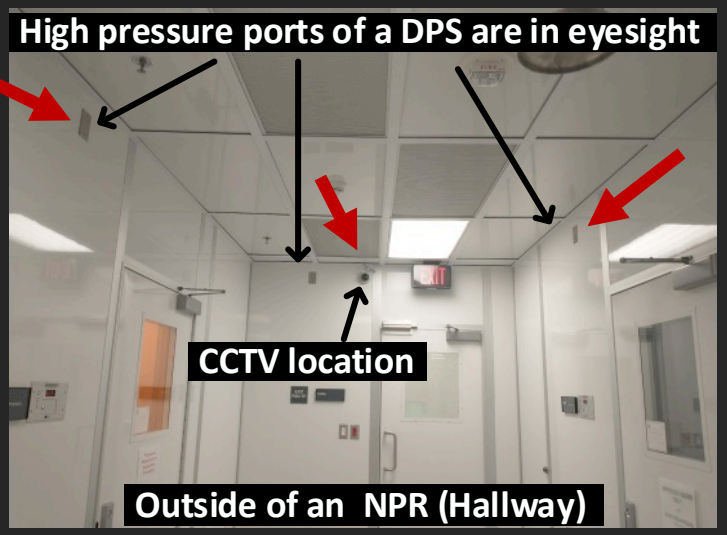






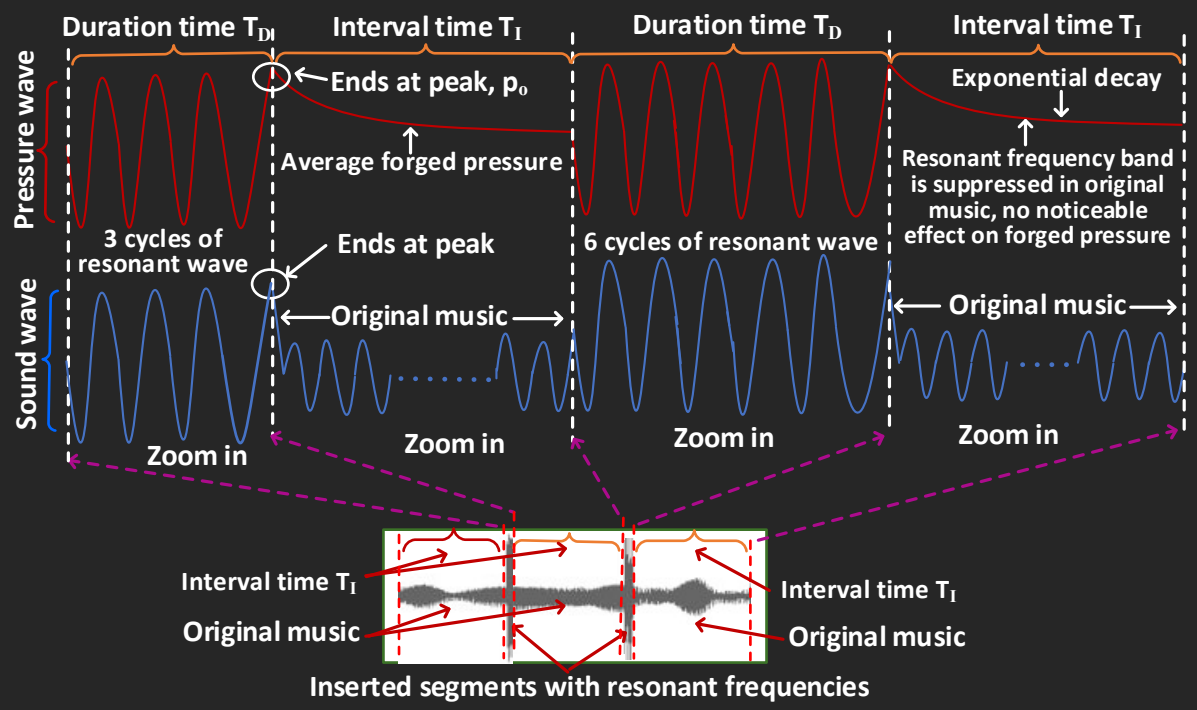
CCTVs with Speakers could be a Source of Attack





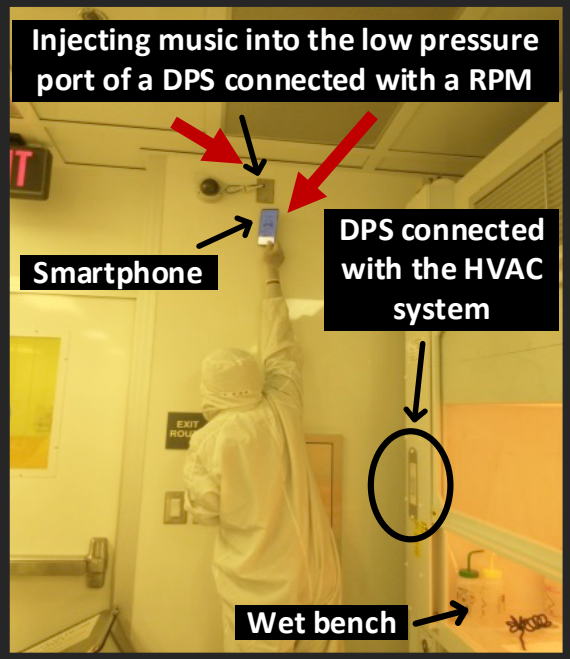
CCTV's locations are very close to pressure sensors in a negative pressure room

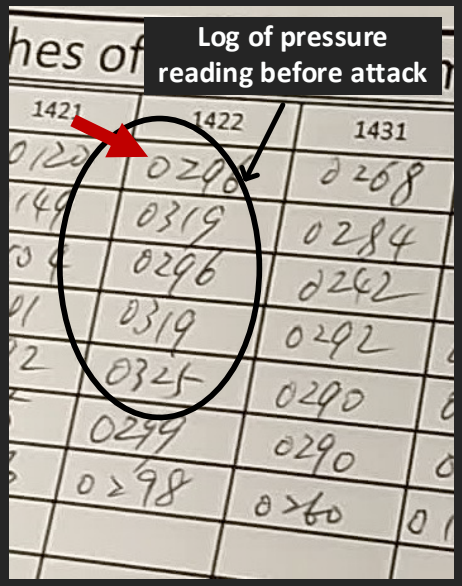
Inserting Resonant Frequency into Music

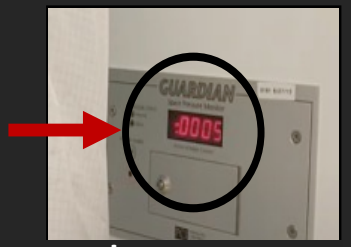


- Authority may ascribe this as a problem in the speaker
- May neglect this issue

Attack Demonstration







-0.0005 in. water column pressure reading after sound injection

Attack demonstration with a cellphone in a negative pressure room

Media Coverage

UCI News

UCI researchers demonstrate how to trigger a pathogen release with music

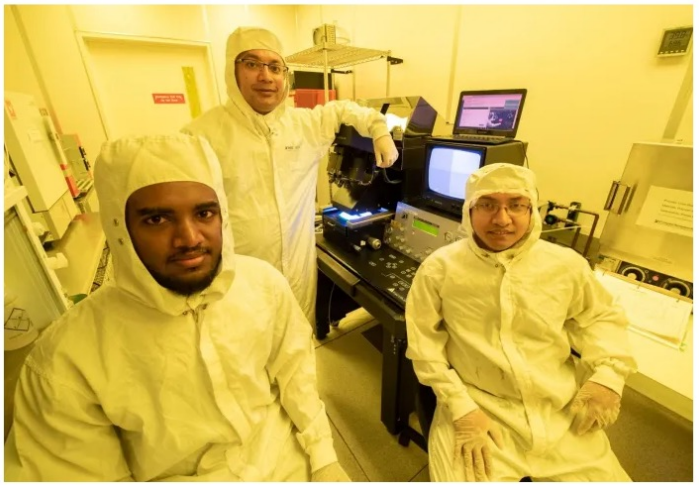
Hospital and laboratory biocontainment facilities vulnerable to terrorist attack

November 17, 2022

Researchers discover how music could be used to trigger a deadly pathogen release

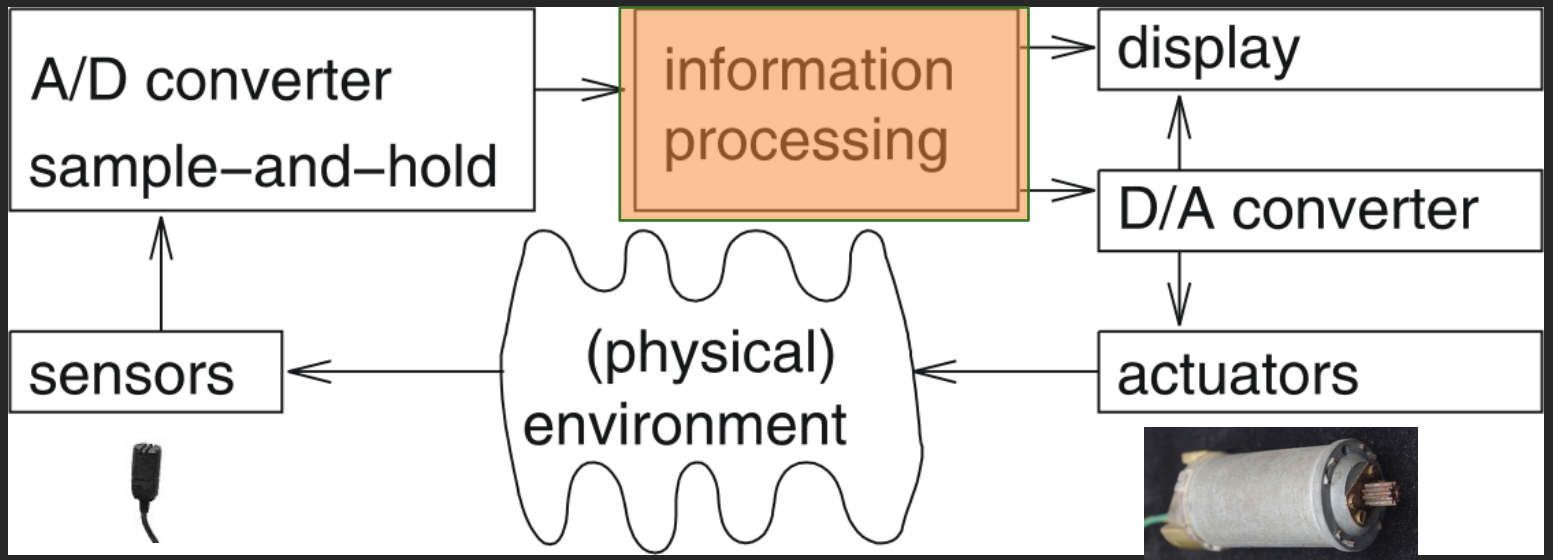
By **News8Plus** 18th November 2022 27 0

Share



Abstract View of an Embedded Systems/CPS/Control System

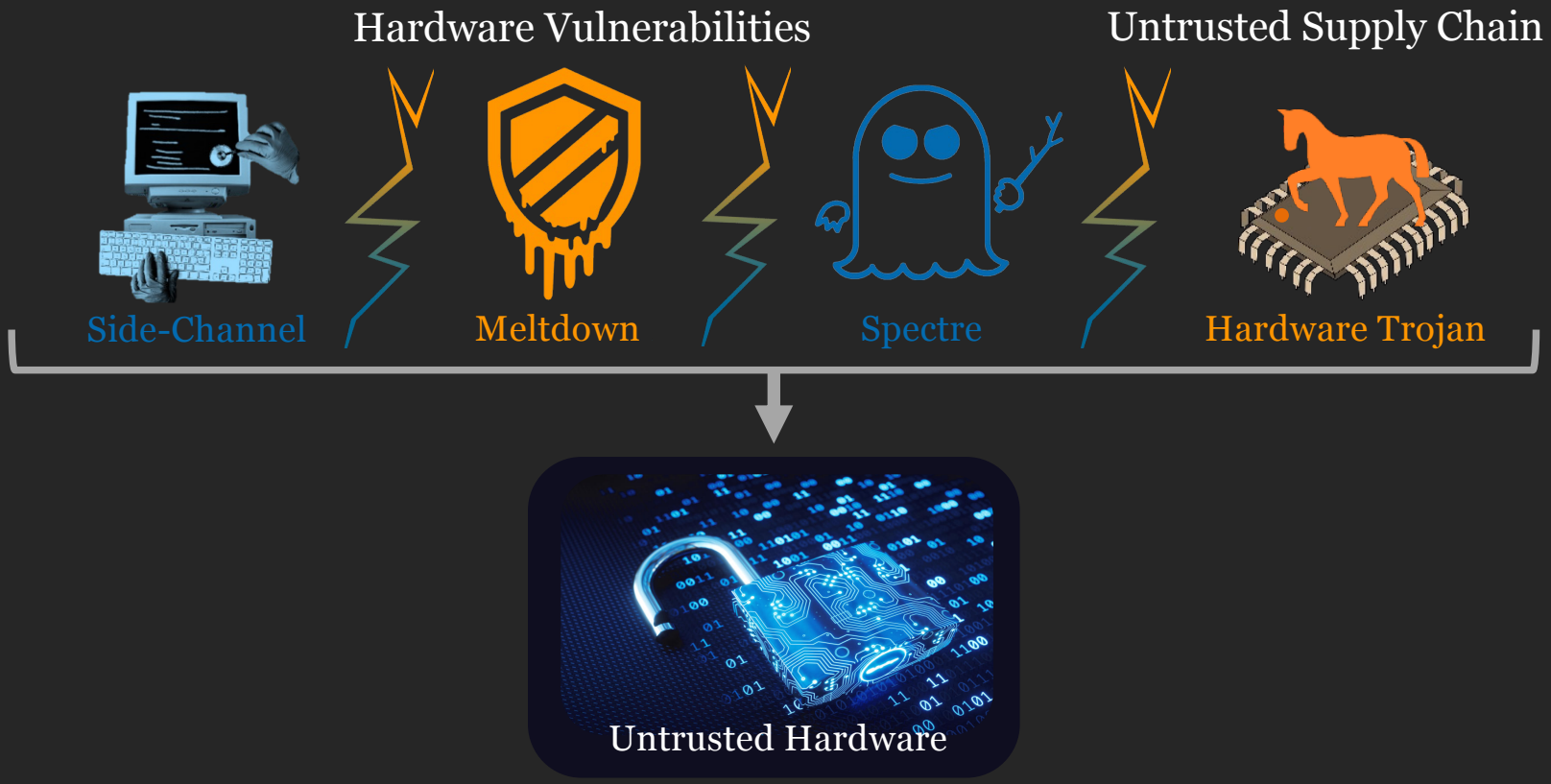
- cyber-physical systems



Hardware is not Trusted anymore!

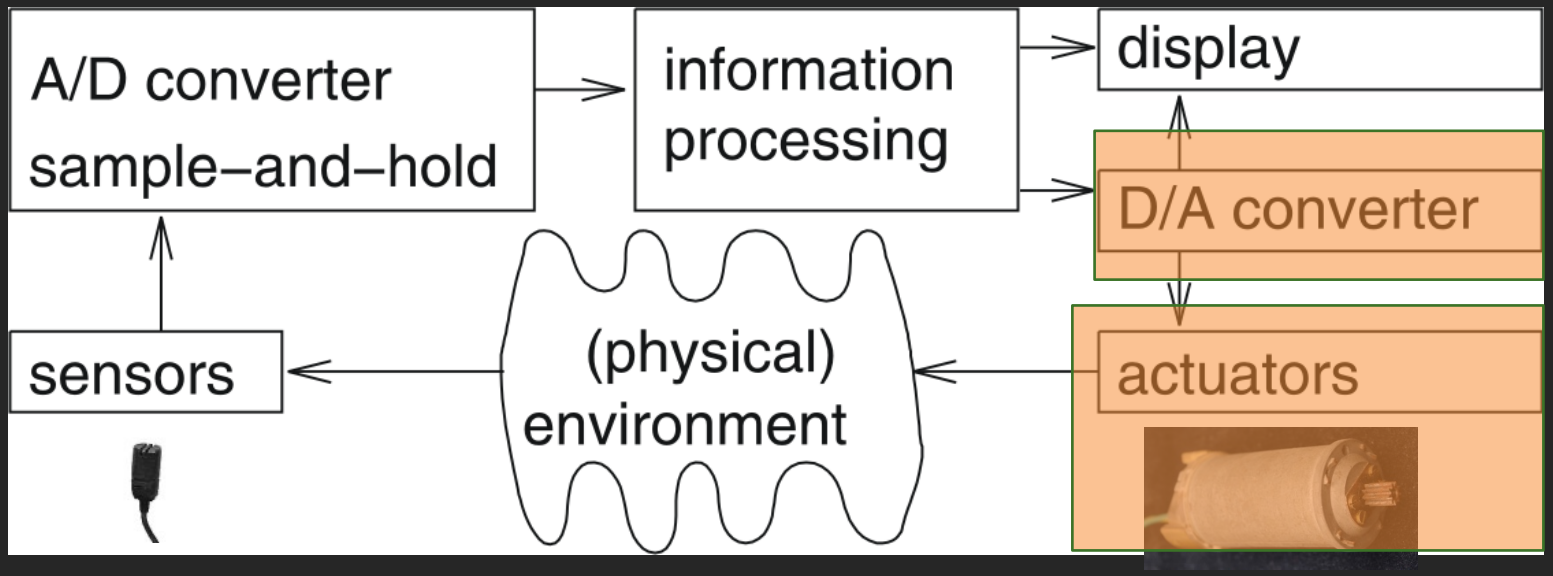
- Existing cyber security measures assume trusted hardware
- Hardware is not trusted anymore.

Untrusted Hardware

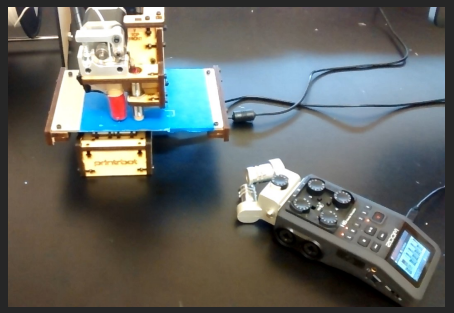


Abstract View of an Embedded Systems/CPS/Control System

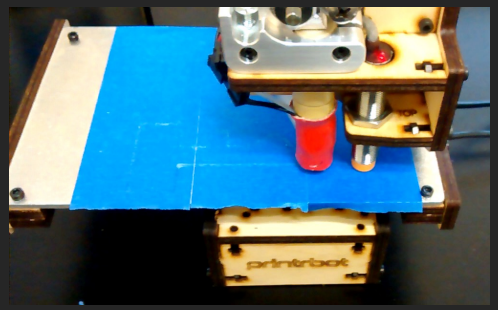
- cyber-physical systems



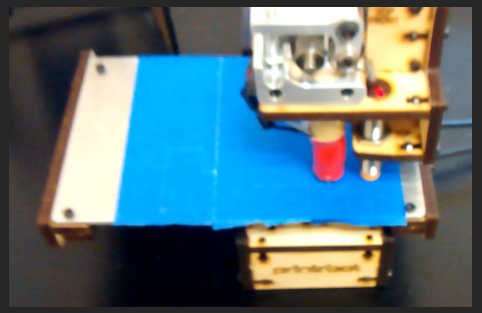
Attack on a 3D Printer – Physical2Cyber Attack



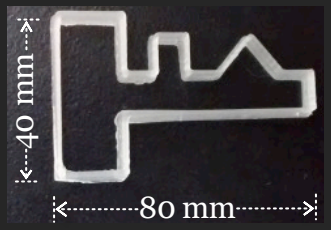
Outline of a Key Being Printed



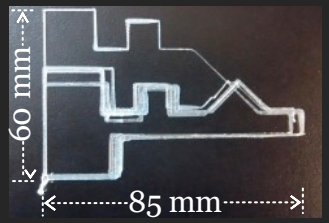
Reconstructed Object Before Post Processing



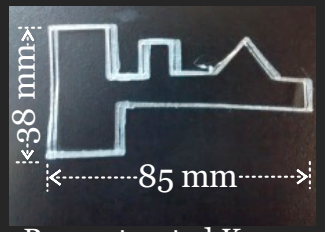
Reconstructed Object After Post Processing



Original 3D-Printed Key



Reconstructed Key Before Post Processing

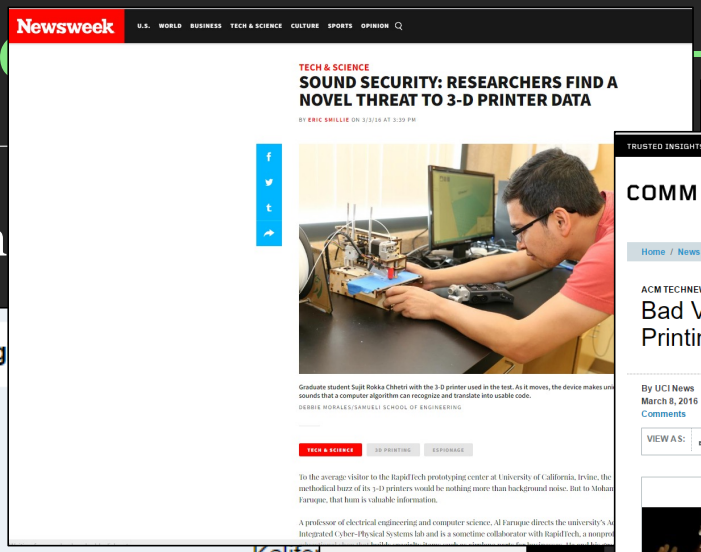


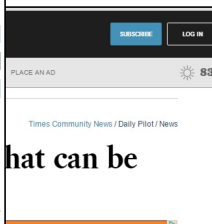
Reconstructed Key After Post Processing

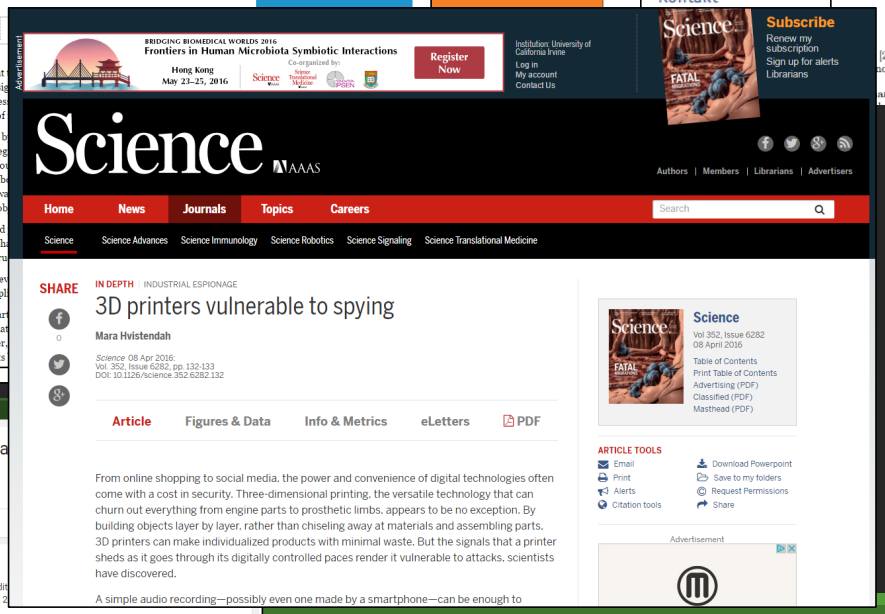
- **Perimeter accuracy after post processing: 89.72%**

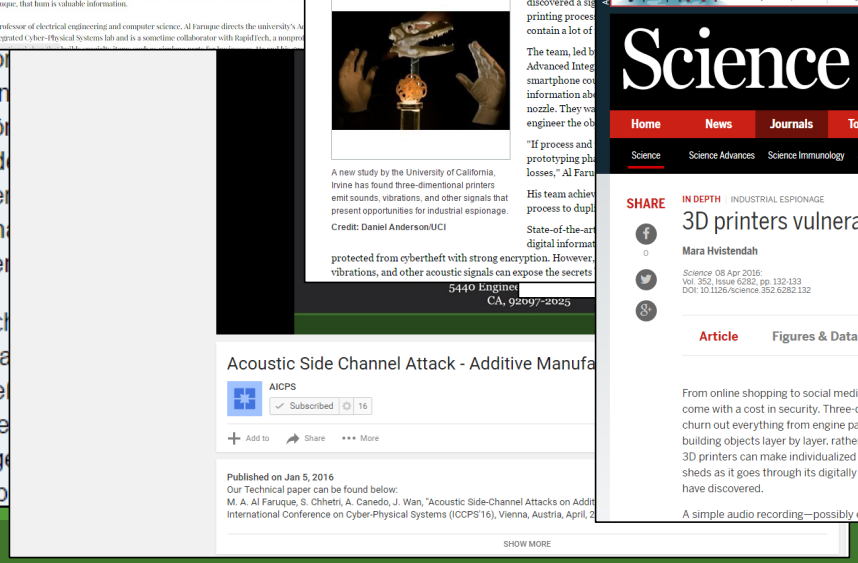
Attac – Physical2Cyber Attack

- In
  - Dig
  - Kalifor
  - anhan
  - herkö
  - gerad
  - Siche
  - Interna
  - Syste
  - Schich
  - Einma
  - schlie
  - entste
  - hier g
  - Comp



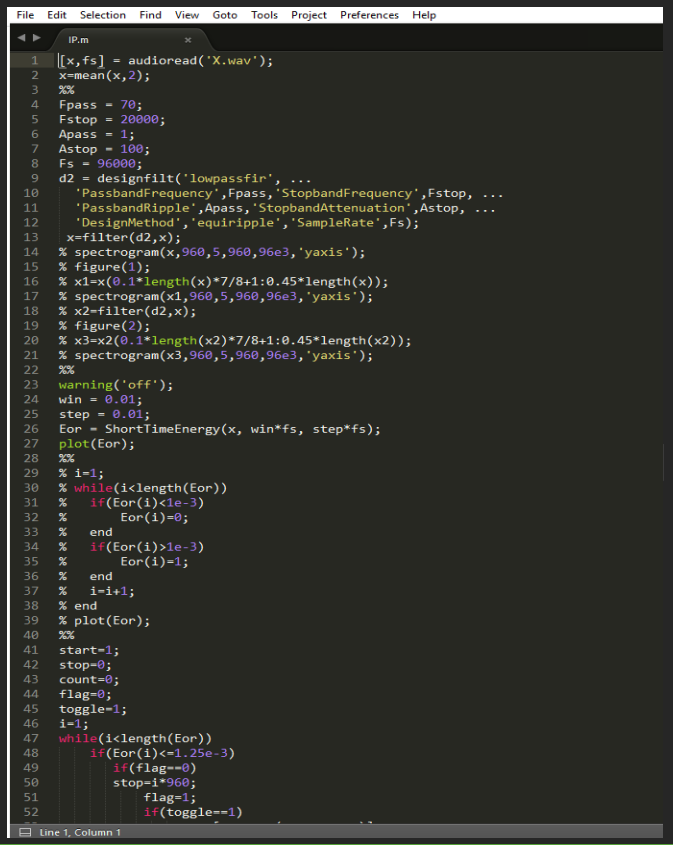






Intellectual Property (IP)

- Unique Features
- IP in Additive Manufacturing [1]
  - Geometric Shape,
  - Process Information,
  - Machine Information,
  - Stored in Cyber Domain!



[1] M. Yampolskiy et al., "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in Proceedings of the 4th Program Protection and Reverse Engineering Workshop, p. 7, **ACM, 2014.**

Attack on a DNA Synthesis Machine– Physical2Cyber Attack

Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines

Sina Faezi*, Sujit Rokka Chhetri*, Arnav Vaibhav Malawade*, John Charles Chaput*, William Grover†, Philip Brisk†, and Mohammad Abdullah Al Faruque*
*University of California, Irvine, Email: {sfaezi, schhetri, malawada, john.chaput, alfaruqu}@uci.edu
†University of California, Riverside, Email: wgrover@engr.ucr.edu, philip@cs.ucr.edu

***Abstract*—Synthetic biology is developing into a promising science and engineering field. One of the enabling technologies for this field is the DNA synthesizer. It allows researchers to custom-build sequences of oligonucleotides (short DNA strands) using the nucleobases: Adenine (A), Guanine (G), Cytosine (C), and Thymine (T). Incorporating these sequences into organisms can result in improved disease resistance and lifespan for plants, animals, and humans. Hence, many laboratories spend large amounts of capital researching and developing unique sequences of oligonucleotides. However, these DNA synthesizers are fully automated systems with cyber-domain processes and physical domain components. Hence, they may be prone to security breaches like any other computing system. In our work, we present a novel acoustic side-channel attack methodology which can be used on DNA synthesizers to breach their confidentiality and steal valuable oligonucleotide sequences. Our proposed attack methodology achieves an average accuracy of 88.07% in predicting each base and is able to reconstruct short sequences with 100% accuracy by making less than 21 guesses out of 4^{15} possibilities. We evaluate our attack against the effects of the microphone's distance from the DNA synthesizer and show that our attack methodology can achieve over 80% accuracy when the microphone is placed as far as 0.7 meters from the DNA synthesizer despite the presence of common room noise. In addition, we reconstruct DNA sequences to show how effectively an attacker with biomedical-domain knowledge would be able to derive the intended functionality of the sequence using the proposed attack methodology. To the best of our knowledge, this is the first methodology that highlights the possibility of such an attack on systems used to synthesize DNA molecules.**

I. Introduction

The ability to rapidly sequence and synthesize DNA has profound implications for society. Large libraries of different DNA sequences play an essential role in genomics research, especially for genetic analysis. Synthetic DNA is poised for widespread consumption if its costs can be lowered dramatically. Based on current trends, the global market for synthetic biology is projected to reach $38.7 billion by 2020 [59]. Beyond biological applications, researchers are beginning to construct DNA-based archival storage systems, which can store up to 215 petabytes of data per gram, with centuries to millennia of endurance if properly stored in a cool and dry environment [53].

Unfortunately, technological advancement often creates new security concerns as technologies mature. To date, the foremost security threat in this field involves the physical safety of synthesized DNA. Present efforts to reduce or eliminate misuse of synthetic DNA include biosecurity regulations, training and licensing programs for authorized agents, and the embedding of screening chips into DNA synthesizers (modeled on parental control of television access) [48], [12], [55]. However, these threat models implicitly assume that the value is inherent in the DNA itself, as opposed to the information that is encoded in the DNA.

Somewhat more generally, the cyber-physical nature of biotechnology workflows creates new security risks, which the corresponding research community has mostly neglected [49]. One recent example is the now-demonstrated ability to encode information into a DNA sequence that can trigger a buffer overflow error in DNA sequencing software; this exploit can be used to inject malware into the computer running the sequencing algorithm [47]. A subsequent concern is the confidentiality of DNA sequences stored in human biobanks. If the genetic information of the earth's population is exposed, then an attacker may be able to create a contagious virus that is fatal to individuals or a small group, but is otherwise benign to the general population [46].

Confidentiality concerns also extend to synthetic DNA sequences. In synthetic biology, the objective is often to engineer an organism with desired traits or functions. Investors only reap the rewards of their investments *after* the engineered organism passes all regulatory requirements and the investor obtains intellectual property ownership in the form of a patent or copyright. However, while the organism is still under development, the research remains vulnerable to industrial espionage or academic intellectual property theft [60]. In this case, the actual secret to be protected may be an amino acid sequence within a protein (which is derived from DNA) as opposed to the DNA itself. Within this larger context, knowledge of the DNA can still help an attacker determine the amino acid sequence, and the attacker can further benefit if he or she has knowledge of the desired traits or functions of the organism under development.

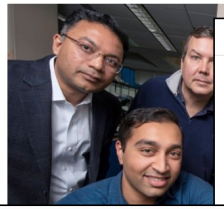
A. Motivation and Overview

This paper presents *Oligo-Snoop*: a novel, acoustic, side-channel, analysis-based attack model that can breach the confidentiality of DNA synthesizers. The attack model leverages the physical implementation of the synthesizer to infer the DNA sequence being synthesized. By publishing this attack, we hope to encourage commercial DNA synthesizer manufacturers to

Network and Distributed Systems Security (NDSS) Symposium 2019
24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X
https://dx.doi.org/10.14722/ndss.2019.23544
www.ndss-symposium.org

The New York Times

U.S. | Is the Next Hacking Frontier Being Developed in California?



The New York Times

CALIFORNIA TODAY

Is the Next Hacking Frontier Being Developed in California?

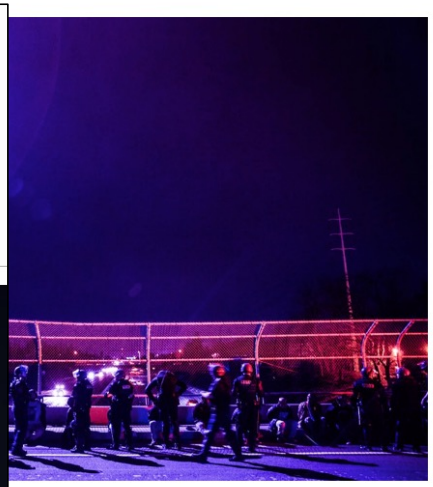
2,071 views | Feb 27, 2019, 07:30am EST

Sound Waves Can Be Hacked For Everything From Ad Targeting To Bioterrorism

Jessica Baron Former Contributor

Consumer Tech

Jessica Baron is a tech ethicist and a freelance writer and editor.

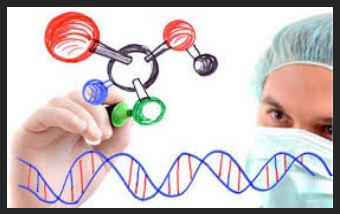


a march through an East Sacramento neighborhood in protest
rge the police officers who shot Stephon Clark. Max Whittaker

Motivation: A Different Perspective

- Synthetic DNA market $38.7 billion by 2020 [2].

Drug Discovery



Medical Treatment

Crop Optimization

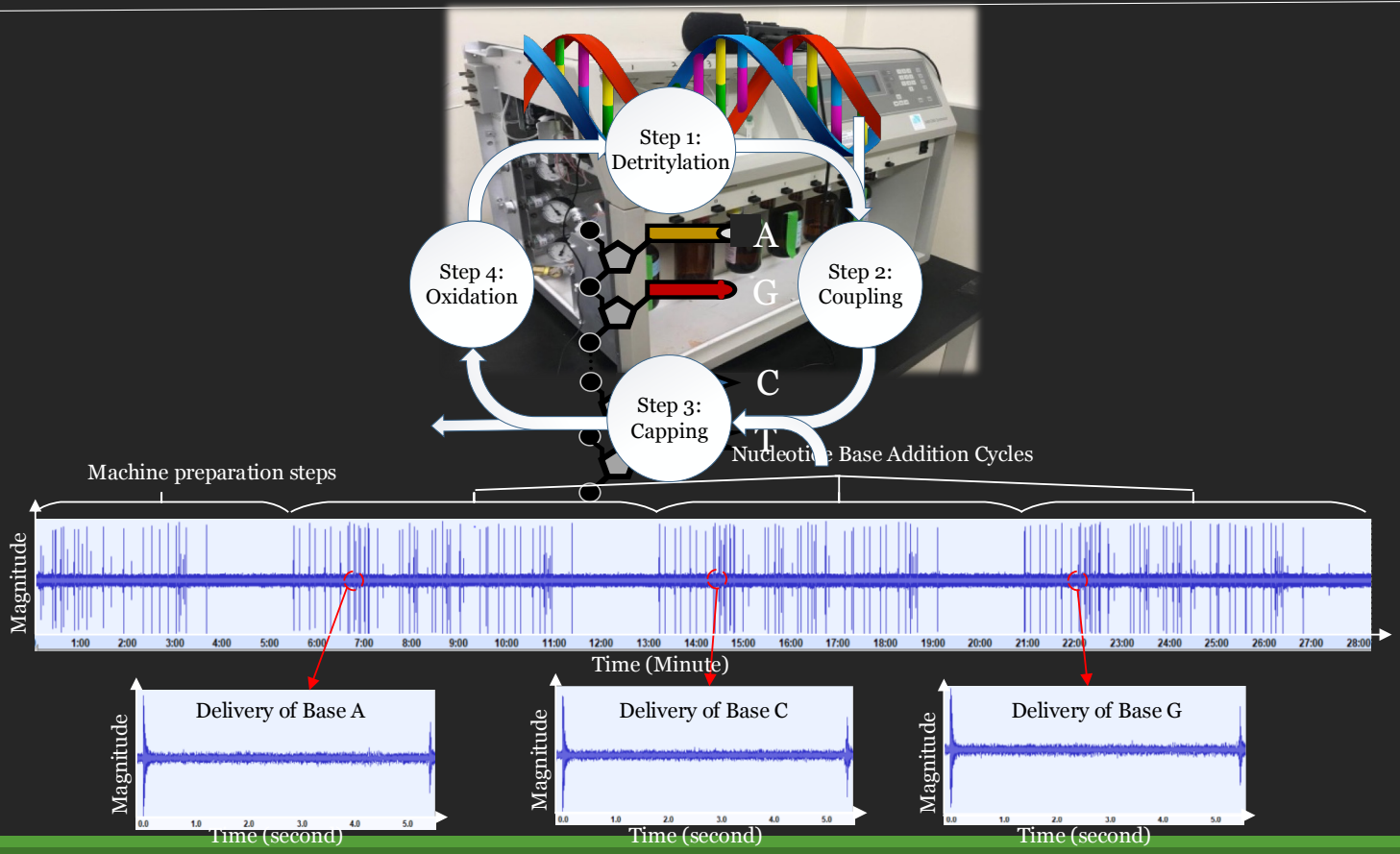
AGGCAGGTTTTCTAGCTGGAACTCCGA

Synthetic DNA Sequences are Intellectual Properties.

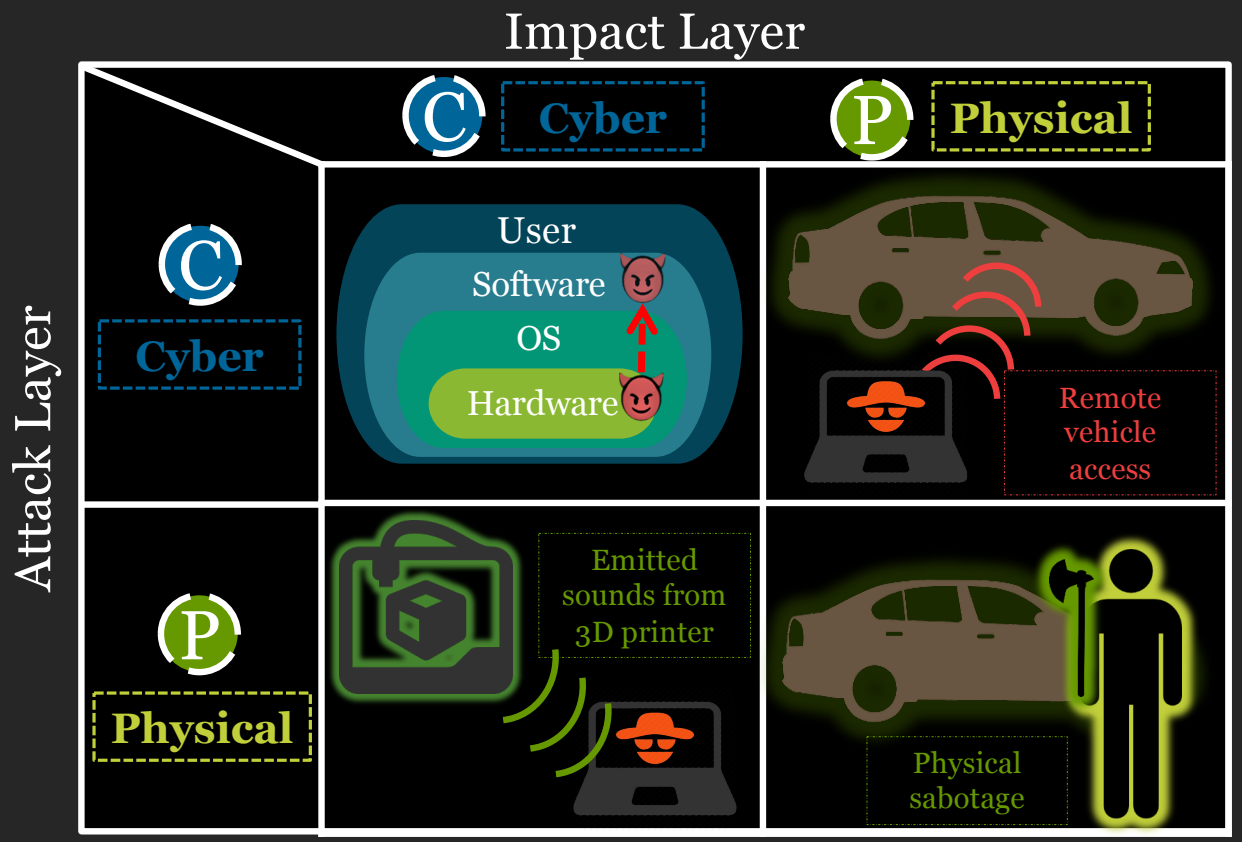
IP ($$$)

[2] Ranjan Singh. 2014. Synthetic Biology Market by Products and ,Global Opportunity Analysis and Industry Forecast, 2013 - 2020. (2014).

DNA Synthesizer



Cross-Layer Security in Embedded & Cyber-Physical Systems



Take Away from the Talk

- Cross-layer security threats are real!
- Hardware is not trusted anymore.
- Physical Environment can not be trusted anymore!
- Cross-layer may span multiple layers → P2C2C2P2C
- Security should be considered as a first-class design criteria
- Domain knowledge needs to be considered → Multi-disciplinary
- Defenses must consider cross-layer techniques!

Questions

Autonomous and Intelligent
Cyber-Physical Systems Laboratory

Thank You for Your Attention

Contact Email: alfaruqu@uci.edu