TOWARDS A CYBER-PHYSICAL FUZZING SIMULATION FRAMEWORK

Presenter: Jasmine Unterburger
(junterbu@isi.edu)

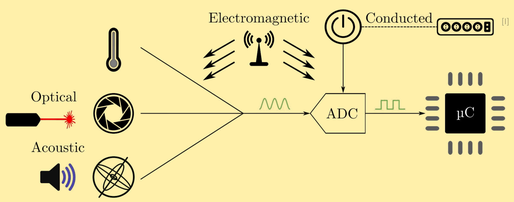
Mentor: Luis Garcia
(lgarcia@isi.edu)

MOTIVATION

• Malicious attacks and exploitation of hardware vulnerabilities within a device.

Cyber-physical systems depend heavily on their sensor's and actuator's ability to interpret their surroundings in order to make decisions. Thus, having existing hardware imperfections makes you highly susceptible to security risks.

Recent research has shown how a wide range of everyday devices and sensors can be targeted by out-of-band signal attacks due to inherently vulnerable hardware. Although many have performed studies on physical devices rather than in simulation and often times have abstracted away analysis of realistic dynamics.



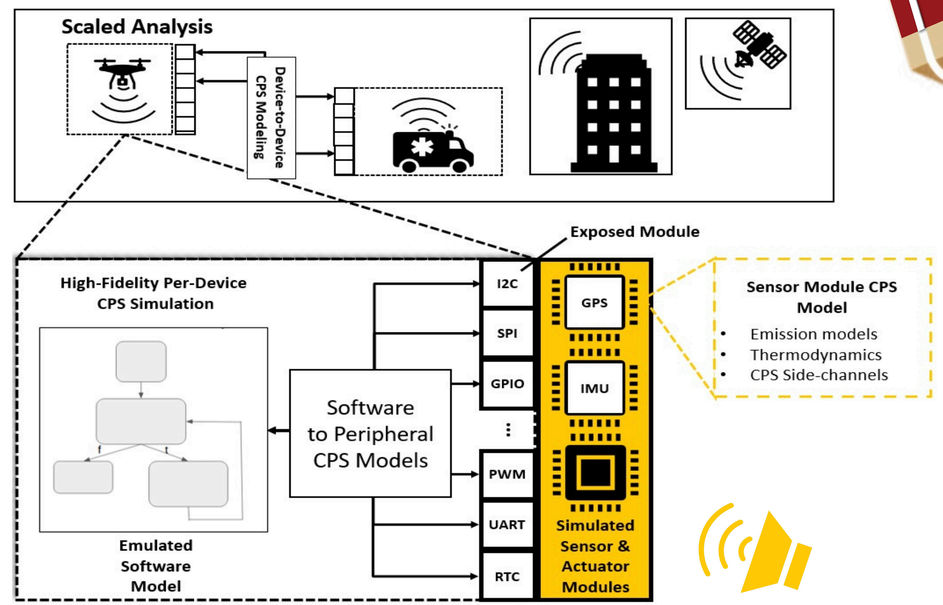
These influences and the increasing dependence on sensor and actuators emphasizes the need for a directed model that focuses on building a method to avoid threats before devices are deployed.

Recent Attacks

• Smart Bulbs hacked by infrared light emissions

• Smartphone's Microphone Used to Launch Acoustic Side-Channel Attack

DESIGN



IMPLEMENTATION

• We are examining the security and integrity of a drone's sensor to actuator connections in simulation without abstracting away its dynamics.

In particular, we propose modeling a drone as a cyber-physical system, including capturing the full dynamics of its sensor to actuator interactions, which are composed of smaller cyber-physical systems. By simulating the sensor and actuator models, we can then using signal generators to perform cyber-physical fuzzing to assess when a sensor is disrupted.

These attack techniques can be performed on a wide range of sensors using several different signals— electromagnetic radiation, acoustic waves, optical emissions, etc. In our approach, we are initially focusing on the inertial measurement unit, specifically the microphone, against acoustic signals.

CHALLENGES

• Integrating sensor and actuator dynamics for a drone in simulation

• How to capture its physical dynamics & how it interacts with its cyber components and environment.

• (Long-term) How to ensure the physical & cyber components are both synchronized on the same instance of time. Possibly with the help of the Cypress testbed.

• (Long-term) How to accomplish simulation at scale with high fidelity

CURRENT STATUS

• Assessing the feasibility of capturing a signal sensor to actuator within the same modality.

• Insert acoustic signals in simulation to evaluate when an expected interaction occurs and how that affects the drone.

• Begin capturing the vulnerabilities for this particular sensor.

• Begin by capturing all side channels or attacks for one particular sensor

• Try to model interference across different modalities

• This can enable opportunities to build a model for exposing out-of-band sensor vulnerabilities

FUTURE DIRECTION

By assessing the security in simulation, we are able to use signal generators against a drone's sensors and actuators to highlight when there is an expected interaction and how it will affect the drone. With this approach, we will be able to effectively replicate experiments with ease and accommodate for crucial physical dynamics.

Long term, we expect this will allow us to create and integrate a sensor model with a full simulation framework for detecting and predicting hardware vulnerabilities before being deployed.

Work performed under REU Site program supported by NSF grant #2051101

1. Giechaskiel and K. Rasmussen, "Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 645-670, Firstquarter 2020, doi: 10.1109/COMST.2019.2952858. 2. vecteezy