CS 6963/5963
University of Utah

Cyber-physical Systems and IoT Security

Module 1a: Course Overview + Logistics

I'm looking for RA's!

Luis Garcia

https://lagarcia.us

My Research: CPS/IoT Security, Safety, & Privacy, XAI for Sensor data, Medical IoT

U of U
Asst. Prof. (Since July)

USC, ISI
Research Lead (2020-2023)

UCLA
Postdoctoral Fellow (2018-2020)

Rutgers
Ph.D.

U of Miami
M.S. + B.S.

Other Course Staff

TA: Ruth **(my dog; no official TA for this course)**
Office Hours: By appointment via e-mail
E-mail: N/A (doesn't trust the internet)

Activities

Join by Web **PollEv.com /luisgarcia307**

What are cyber-physical systems anyways?

Our society increasingly relies on cyber-physical/IoT autonomy…

From safety-critical infrastructure…

…to making our lives more efficient…

...sometimes at odds with security...

A New Era of Internet Attacks Powered by Everyday Devices

By DAVID E. SANGER and NICOLE PERLROTH OCT. 22, 2016

...sometimes at odds with safety...

Driverless Cars Face Setbacks In San Francisco—Here's What To Know About The City's Problematic Robotaxi Rollout

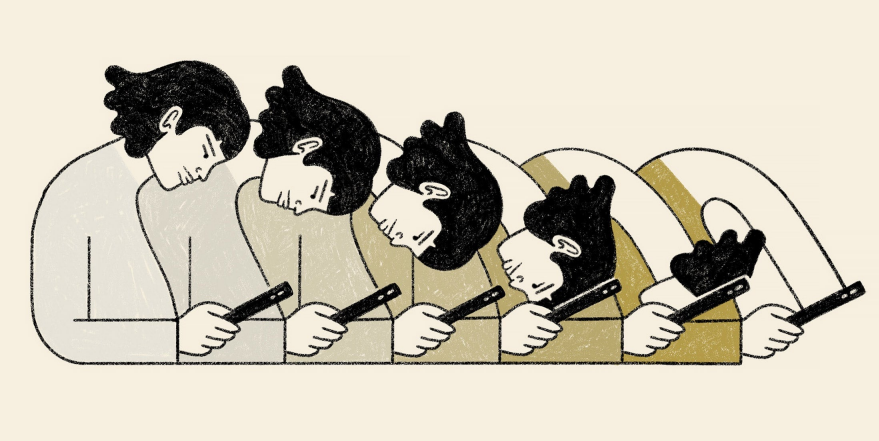
Mary Whitfill Roeloffs Forbes Staff

I am a Boston-based reporter covering breaking news.

Wing delivery drone crashes into power lines in Australia

By Brianna Wessling | September 30, 2022

...sometimes at odds with privacy



Phones That Can Read Your Mind

Targeted ads may soon show you what you really want before you knew you did.

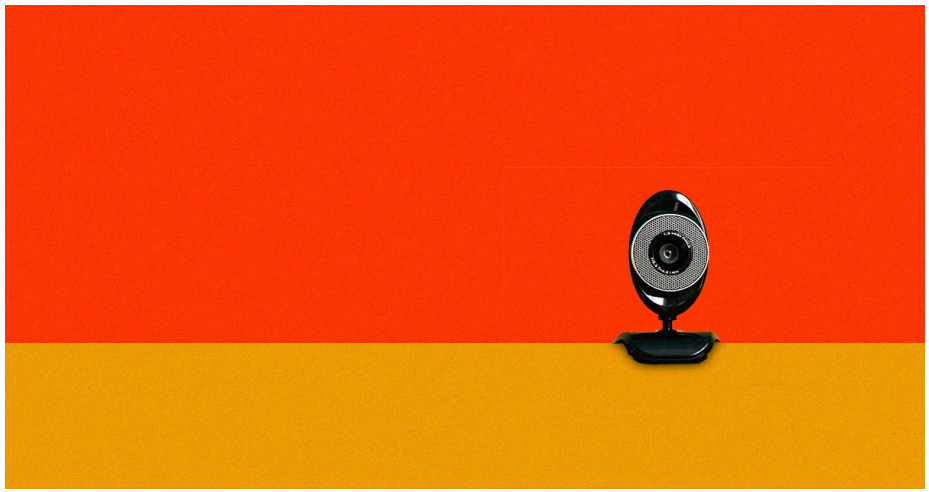
By Andy Kessler Follow

Jan. 26, 2020 3:51 pm ET

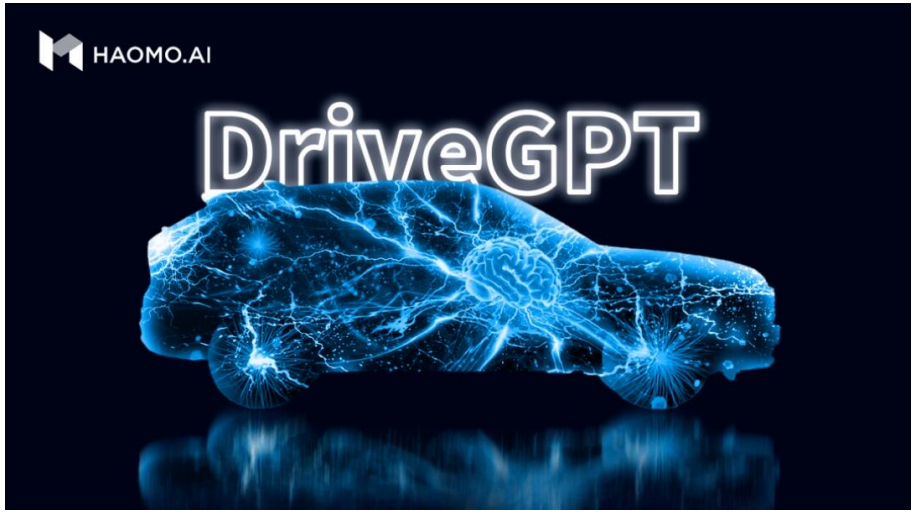
Airbnb Hosts Are Spying on Guests With Hidden Cameras

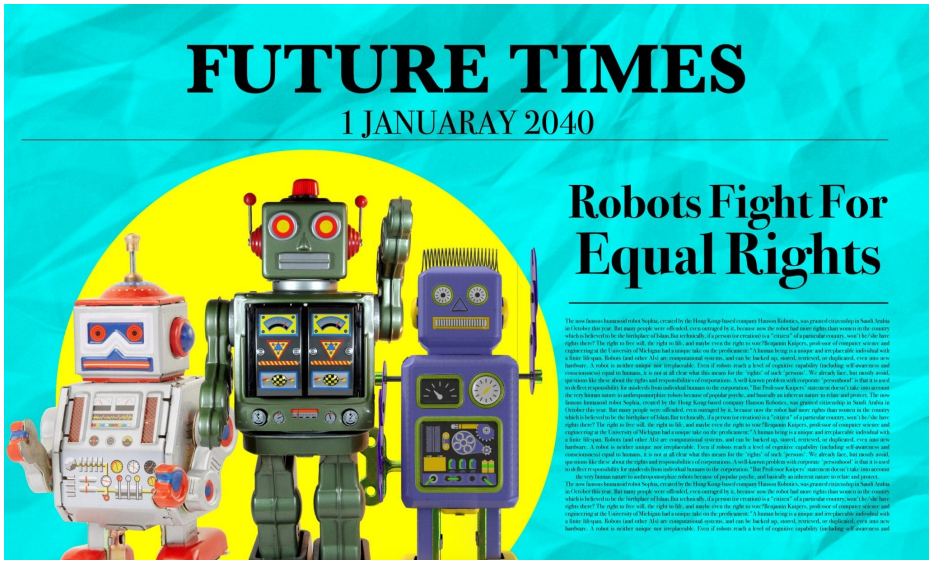
And the platform's botched handling of the issue puts guests in harm's way.

/ Future Society / Airbnb / Gig Economy / Hidden Camera



Innovation only leads to more questions...



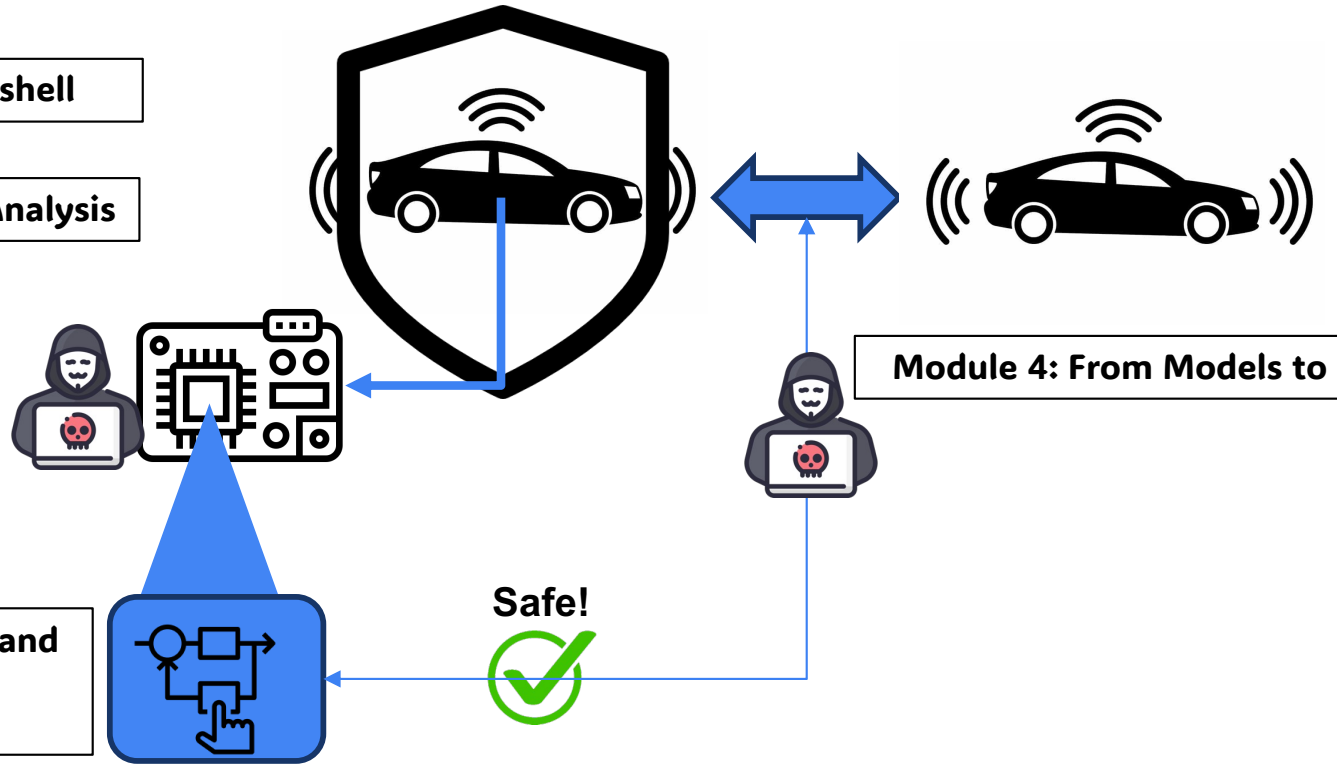


Black-box models == black-box guarantees?

Topics covered in the first half of this course*

Module 1: Security in a nutshell

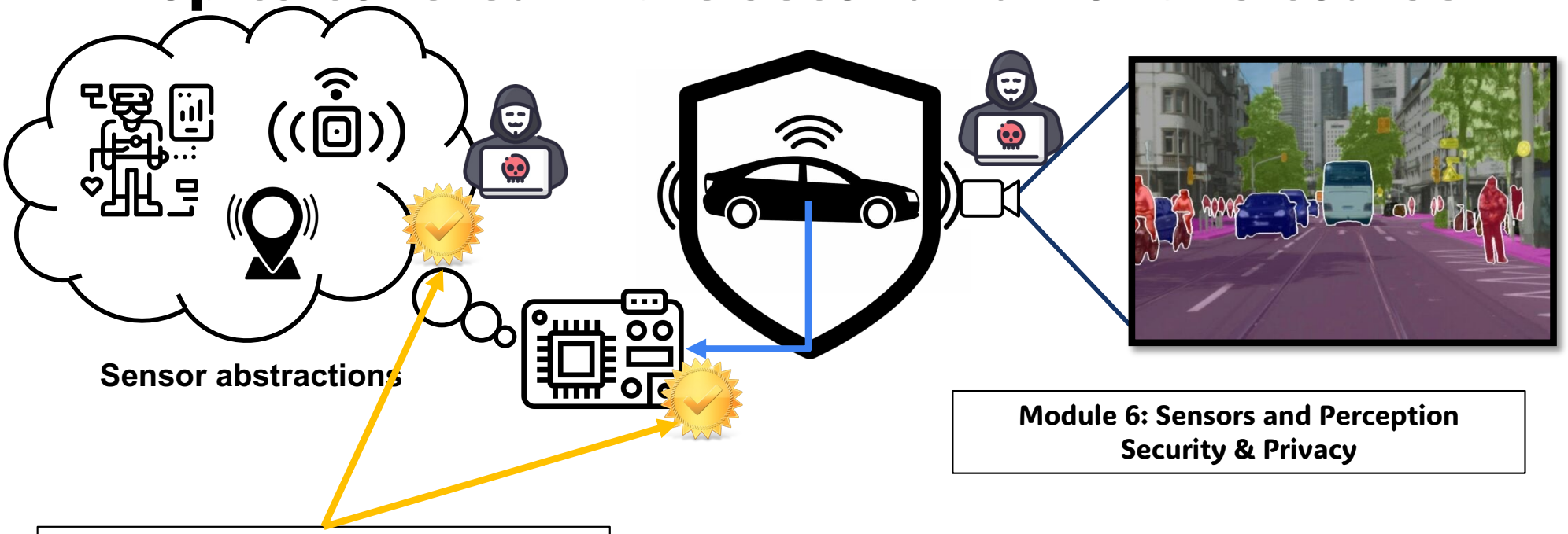
Module 2: CPS/IoT Program Analysis



Module 4: From Models to Exploits

Module 3: Formal Modeling and Verification of CPS

Topics covered in the second half of this course*



Module 6: Sensors and Perception Security & Privacy

Module 7: Establishing Trust for CPS

- Trusted computing/Hardware Support
- Remote Attestation
- Explainable and Verifiable Inferences

Format

- **Meetings:** Tuesdays & Thursdays 12:25 PM-01:45 PM
  - **SFEBB 5180**
- **5 min:** quizzes
  - Not for every class; I'll let you know ahead of time
- **40 – 60 min:** instructor-led lecture
- **20 - 30 min:** student-led paper presentations & discussion
  - Usually 10-min presentations followed by 10-20 min of questions/discussion

Schedule

- Weeks 1 – 2: Introduction and Overview [Module 1]
- Week 3: CPS/IoT Program Analysis [Module 2]
- Weeks 4-5: Formal Modeling and Verification of CPS [Module 3]
- Week 6: From Models to Exploits [Module 4]
- Weeks 7-9: Capture-the-Flag Prep and Execution [Module 5]
- Weeks 9-12: Sensors & Perception Security [Module 6]
- Weeks 12-13: Establishing Trust for CPS [Module 7]
- Weeks 14-15: CTF 2 Prep and Execution [Module 8]
- Week 16: Final Project Presentations

Course Pre-requisites

- Req. 1: *Interest* and *initiative*
  - Work on topics in security, safety, and privacy that excite you!
  - Willingness to learn across several disciplines!

- Req. 2: *background knowledge*
  - I expect most of you to have gone through most of some form of an undergraduate CS/ECE/CE program
  - We'll do a primer on most topics, but it helps to have a computer/network systems background and vague familiarity with security concepts

- Req. 3: *skills*
  - You will be programming, but the projects/assignments will be tailored to your programming background
  - Ability to communicate ideas (presentations, reports)→ we'll work on it though!
  - Make sure to have the necessary skills to support your project (more on that later)

Course Components and Grading

Course Project	*Team*	40%
Paper Presentation	*Individual*	5%
Capture-the Flag Exercises (in-class)	*Team*	20%
Homework Assignments	*Individual or Team*	15%
Attendance	*Individual*	5%
Quizzes	*Individual*	5%

Homework Assignments

- 2 relatively easy labs
  - Details on Canvas
- Paced with content leading up to CTFs
- Can be done in teams for research/problem-solving, but everyone needs to submit their own assignment on Canvas
- **Each homework is due the day we start prepping for the CTFs**

Attendance

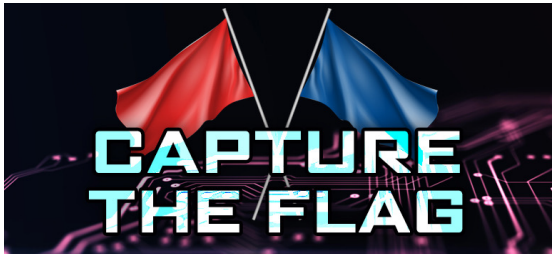
- **Req. 1: Show up to every class**
  - Contact me ahead of the class in case of excused absences
  - We'll have quizzes and polls in class
- **Req. 2:** Participate during other students' presentations
  - Ask thoughtful questions
  - **Help your classmates learn**

Quizzes

- Will be done in the first 5-10 minutes of class
  - The quiz will be available at the start of class, and when you start the quiz, you'll have 5 minutes to complete, and it will not be available after 15 minutes of class
- 1-2 easy multiple choice questions that will be common sense if you paid attention the previous lecture
  - They will not be cumulative
- Not every class, but most likely every other class
  - I'll let you know ahead of time along with the topic

Capture-the-flag Competitions

- 2 capture the flag competitions throughout the course
  - They will be **cyber-physical** in nature
  - They will apply course content
- The homework assignments will build the necessary skills for the CTF
- Will work in teams as both attackers (**red team**) and defenders of your system (**blue team**)
  - Each team will submit a 1-2 page writeup a week after on what worked/didn't work, etc.
- Details will be announced 1-2 weeks before each competition in class
  - Will dedicate 1-2 classes to preparing for CTFs
- Various resources to get familiar with traditional:
  - TryHackMe
  - Hack The Box
  - OverTheWire



Paper Presentations

- **Audience:** not required to read the paper
  - Required to participate in discussion
- **Presenters:** your job is to teach us the paper
  - **10 minute presentation**
  - **Prepare a short slide deck** (feel free to customize existing slides)
  - **Present as if it were your paper:**
    - What are the needs/problems/research gaps being addressed?
    - What is the approach?
    - What is the competition?
    - What is the orthogonal benefit of their approach?
    - Be prepared to list pros vs. cons
  - You need to sign up for paper presentations by 8/31
    - I'll send an announcement with the link along with options for each module

Course Project Overview

Grading Breakdown

Proposal Document	5%
Mid-term Project Progress	10%
Final Report/Demo	20%
Final Presentation	5%

Timeline

Week 2	Team member identification
Week 4	Project Proposal Due
Week 7	Mid-Term Project Progress
Final Week	Final Presentation & Report

Team size: 2 (exceptional cases can be made for 1 or 3 people, and grading will be adjusted)

Choosing a Course Project

- Dig deep into a focus area on your own
  - Use our course module topics as a "general area"
- Aim for something concrete and tangible, even if minor
  - Simulation, analysis, software/hardware design, tools, application, in-depth review…
- Project topics
  - Any IoT/CPS security, safety, or privacy related topic is fair game
  - Coming up with a topic is your responsibility
  - Come and discuss project ideas with me
  - **May relate to your research** but should be different from what is already being done or was being planned to be done, and needs to be approved by me
    - you may not reuse work already being done or planned for your thesis
    - you may not collaborate with other researchers in your group
  - I'll provide feedback/approval on the initial project proposal
  - In-depth solo literature review is okay too as a project, but longer report required
- What should be your goal?
  - something useful, err on the side of risky ideas where the results may turn to be negative
  - similar style/quality as a conference paper and talk
  - key is to keep the project simple, and focused
  - aim for high quality!
- Discuss with me if you need access to certain types of equipment

Project Proposal

- Should follow NABC model:

•**N**eed: What problem am I trying to solve? Why is this problem important? Why is solving it difficult?
•**A**pproach: What is my solution (high level intuition)? What are the details that I have to decide (thresholds, design flow, etc)? How can I reason about these decisions? What data can I use to test my solution? Do I have enough data? Is there noise? Do I understand ground truth? Can I generate synthetic data? What is my desired outcome at the end of the program? What is the smallest unit of work that I can complete to feel I've made progress on solving this problem? You should include a timeline of expected results that fits the course schedule.
•**B**enefit: like the need, but not the same; usually more specific ·or sometimes side-benefits not directly pertaining to need, but nice never the less
•**C**ompetition: review of related work (not exceeding 30% of the presentation); What has been done before (to solve that same problem, to solve related problems that I can leverage)? How do I compare to other efforts to solve that same problem - is my solution better and how? Take a look at a video here for an awesome overview on how to keep track of related works

Course Project Presentations

- **Midterm Presentation (Week 7)**
  - 10 minutes reporting on project
  - Should follow NABC model (more in-depth than project proposal with preliminary findings)

- **Final Presentation (Last Week)**
  - 10-20 minutes depending on time constraints
  - Should include the following
    - Summary of problem definition and solution
    - Key results and findings
    - Conclusions and related work

Course Project Report

- Due by 11:59 PM the day of our final
- 8-10 pages, single-spaced
- If you wish to submit to formal proceedings (conference, journal, etc.), I can provide guidance
- For all team projects, the students will include a separate, brief document describing each team member's contribution
  - All members will "sign off" on the document (e.g., CC'ing everyone on the email)

Academic Integrity

What is and is not OK

- I encourage you to talk with others if you have questions, and to look for answers online, but everyone must DO their work ALONE for specific projects
- Do not turn in the work of others
- Do not give others your work to use as their own
- Do not plagiarize from others (published or not)
- Do not try to deceive the instructor
- If you find answers online, read them, take an hour break and then try to write down the answer without looking back online
- Refer to the Canvas site for more guidelines on academic integrity and links to university resources
- **If in doubt, ask!**

Under no circumstances may you **exploit or misuse** any bugs you find (e.g., zero-day vulnerabilities) for unauthorized access or other illegal activity

Violations of this policy will be referred to Student Conduct

Key Dates

- Aug 22: First Class
- Aug 31:
  - Course Project Team member identification
  - Sign up for Paper presentations (will send out announcement with link)
- Sept. 7: Class presentations begin
- Sept 14: Initial Project Proposal Due
- Sept 28: CTF1 Team member identification Due
- Oct 3:
  - HW1 Due
  - CTF1 Prep begins
- Oct 5: Midterm Project Presentations
- Oct 10 – 15: **Fall Break**
- Oct 17: CTF1 (in class)
- Oct 24: CTF1 Report Due
- Nov. 16: CTF2 Team Member identification due
- Nov. 21: HW2 Due
- Dec. 7:
  - Final project presentations
  - CTF2 Report due
- Finals week:
  - Final project reports will be due at 11:59 on the day of our final

Fishing for project ideas?

(Looking at *recent* top conferences)

Fishing for Project Ideas: Looking at recent top conferences (last 2 years)

- Look for CPS/IoT-related projects
- Major Security conferences (decent ranking list)
  - Top 4: CCS, Oakland S&P, USENIX Security, NDSS
- Major IoT/CPS/Mobile Focused Conferences with Security Topics
  - ACM SenSys
  - ACM MobiSys
  - USENIX NSDI
  - Any of the CPSWeek Conferences (ICCPS, IoTDI, HSCC,…)
- Check out co-located workshops

Fishing for project ideas?

(Look at key research groups)

Fishing for project ideas?
Look at key research groups

Navigation tips:

- Research websites
  - Look at current projects, recent pubs, etc.
- Recent pubs (on Google Scholar)
- Recent seminar/talks on YouTube
- Identify *well-supported* open source tools
  - Reproduce their results and find discrepancies
  - Identify tools you can build upon
  - …
- Identify practical applications/problems
  - Datasets/benchmarks used

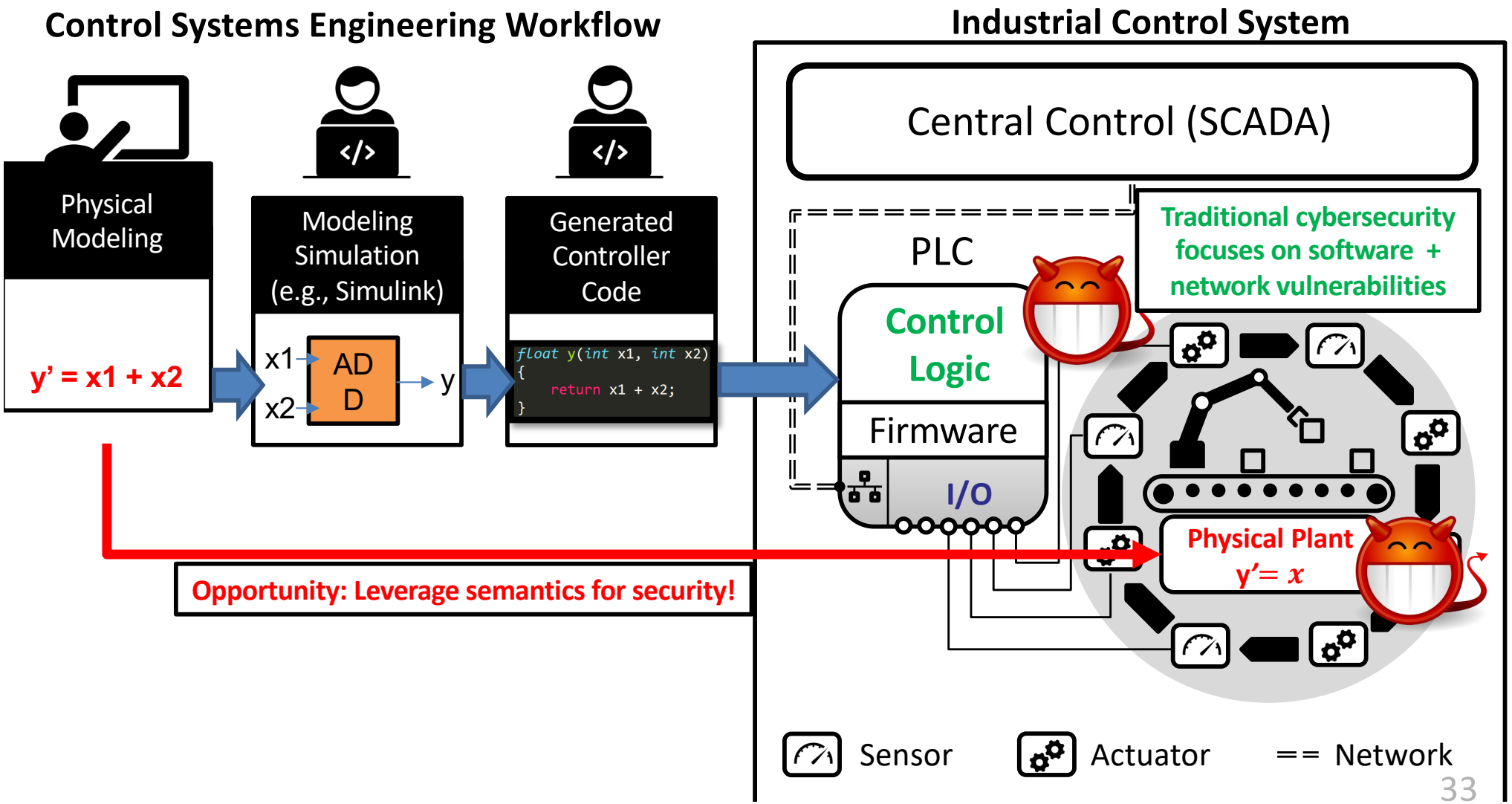
A few big names:

- CISPA: Nils Ole Tippenhauer
- ETH Zurich: Adrian Perrig, Srdjan Capkun
- Georgia Tech: Saman Zonouz, Raheem Beyah
- Stanford: Dan Boneh
- Purdue (CERIAS): Dongyan Xu, Berkay Celik, Dave Tian
- U Arizona: Georgios Fainekos, Giulia Pedrielli
- UCLA: Mani Srivastava
- UF: Kevin Butler
- UC Irvine: Gene Tsudik, Yasser Shoukry, Michael Franz, Sharad Mehrotra, Alfred Chen
- UC San Diego: Hovav Shacham, Earlence Fernandes
- U Michigan: Atul Prakash, Kevin Fu
- U Penn: Insup Lee
- USC: Jyotirmoy Deshmukh
- UT Austin: Todd Humphreys
- UW: Yoshi Kohno, Franziska Roesner
- TU Darmstadt: Ahmad-Reza Sadeghi
- …and many, many more

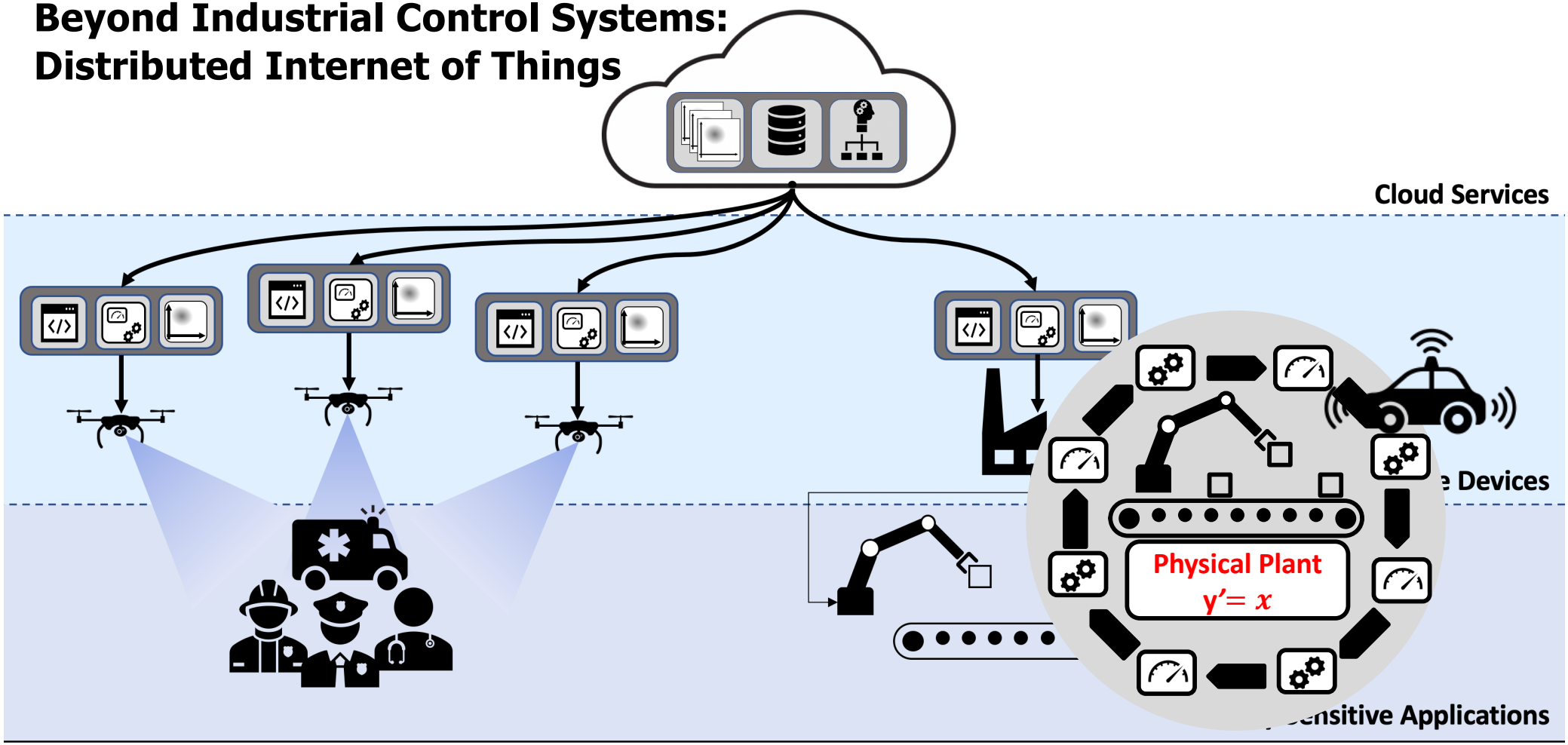
Fishing for project ideas?

(Looking my active research)

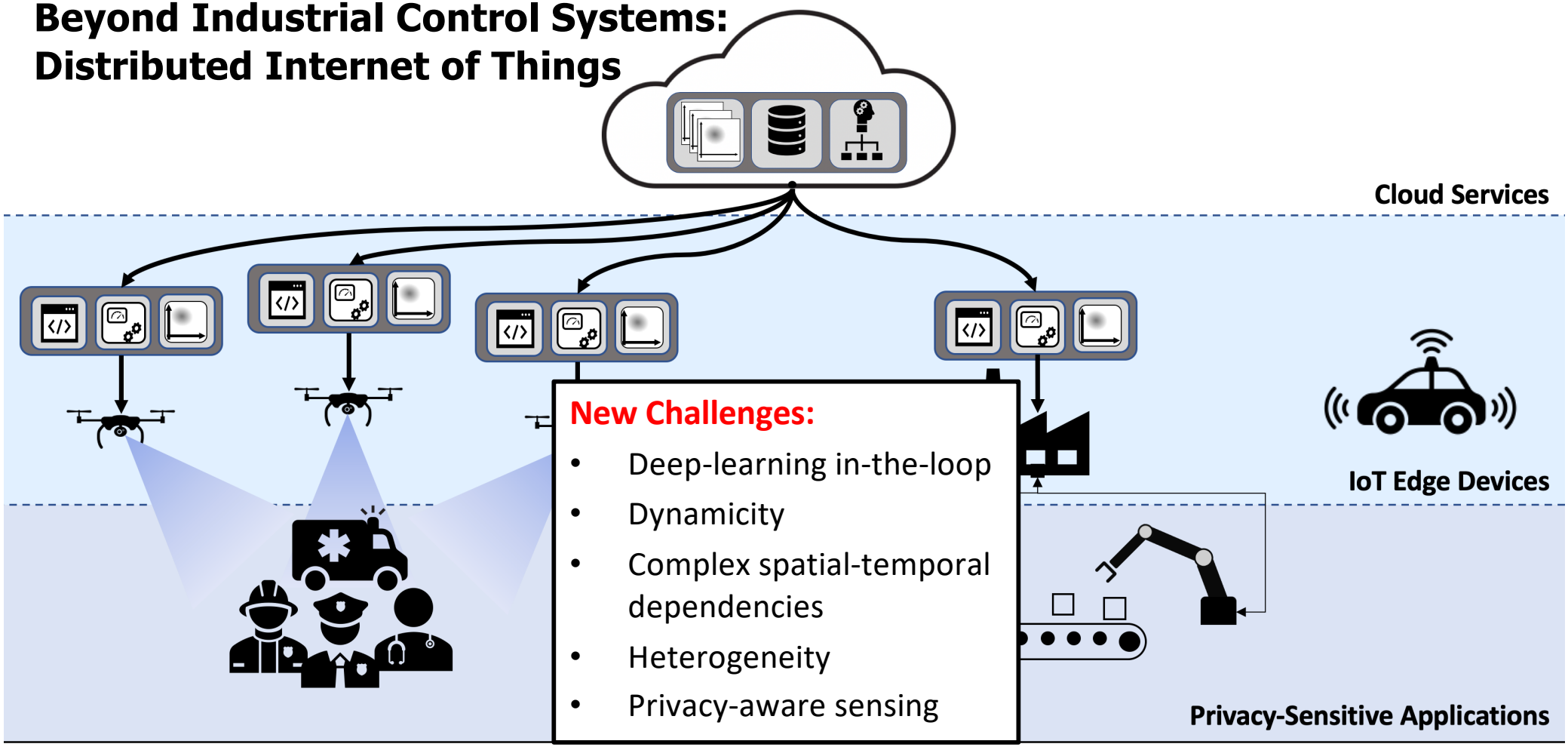
My Research


Control Systems Engineering Workflow
Industrial Control System
Physical Modeling
y' = x1 + x2
Modeling Simulation (e.g., Simulink)
x1
x2
ADD
y
Generated Controller Code
float y(int x1, int x2)
{
return x1 + x2;
}
Central Control (SCADA)
PLC
Control Logic
Firmware
I/O
Traditional cybersecurity focuses on software + network vulnerabilities
Physical Plant
y'= x
Opportunity: Leverage semantics for security!
Sensor
Actuator
== Network

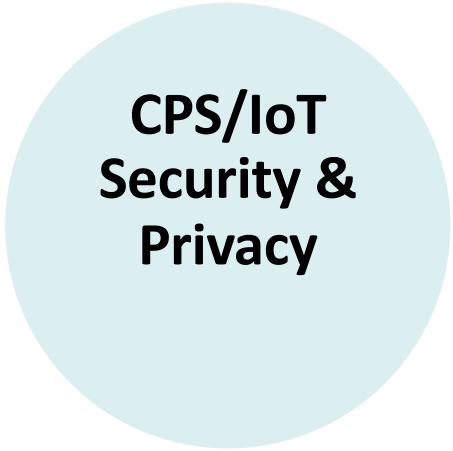
Beyond Industrial Control Systems: Distributed Internet of Things



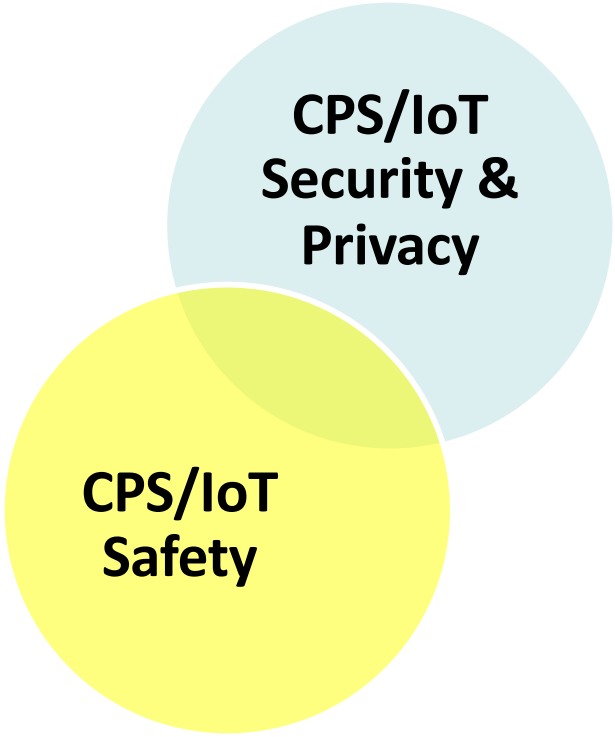
Beyond Industrial Control Systems: Distributed Internet of Things



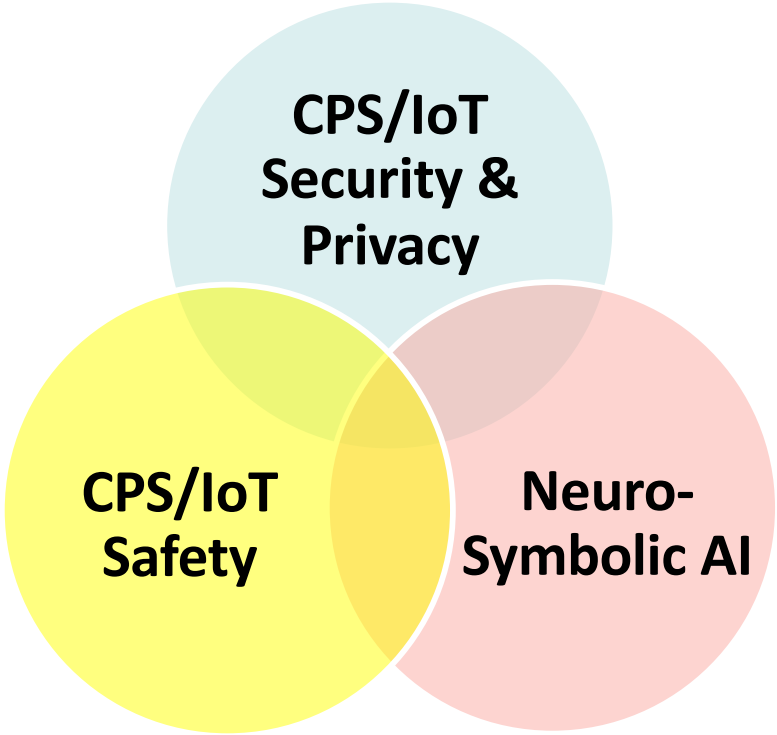
Overview of my Research: PhD



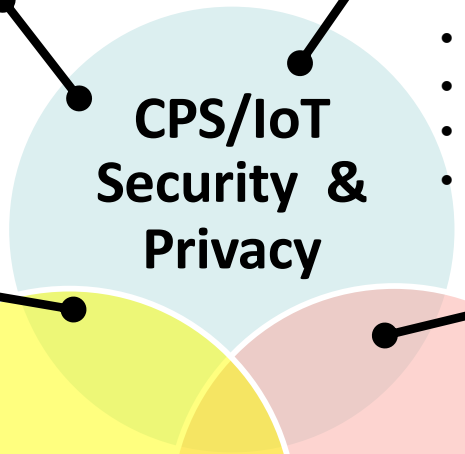
Overview of my Research: PhD



Overview of my Research : PhD + Postdoc and Beyond



Overview of my Research



Information Security & Privacy
- Swirls DSN '16
- SnoopDog USENIX '21
- SecDeep IoTDI '21
- Aerogel SEC '21

Physics-Aware Reverse Engineering + Retrofitting
- Mismo DSN '19
- Patchecko DSN '20
- PERFUME CheckMATE '21
- AutoCPS SafeThings '22
- NS3 NeurIPS '22

Physics-Aware Security
- Harvey NDSS '17
- 3D Printing USENIX '17
- Patt RAID '19
- Scadman ICCPS '20

Privacy-sensitive Data Generation
- PhysioGAN TPAMI '23

Hybrid Systems Modelling
- HyPLC ICCPS '20

Explainable AI
- ExMatchina NeurIPS '20
- XCHAR IMWUT '23
- CoDEx ICLR '23

Macro-programming Abstractions
- Remediot BuildSys '19
- DDFlow IoTDI '19
- Heliot (demo) IoTDI '19

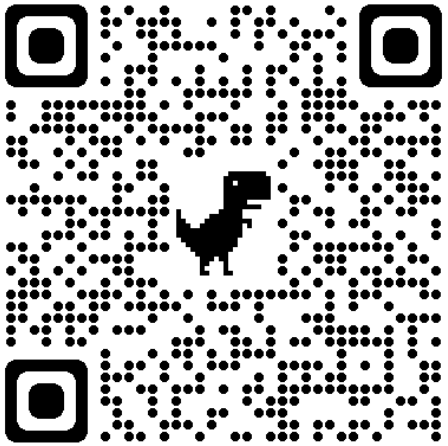
Neuro-symbolic IoT
- NeuroPlex SenSys '20
- DADRL CoRL '21
- DeepSQA IoTDI '21
- TinyOdom IMWUT

Best
Finalist
Under Review

Fishing for project ideas?
some active projects of mine...

1. Trustworthy IoT-in-the-loop Neuroscience
2. Secure Peripheral Abstractions in Cyber-physical Systems
3. Semantic Reverse Engineering of Cyber-physical Systems (Drones)
4. Formal Verification for Industrial Control Systems
5. Privacy Factors for Ubiquitous IoT

Project Descriptions:



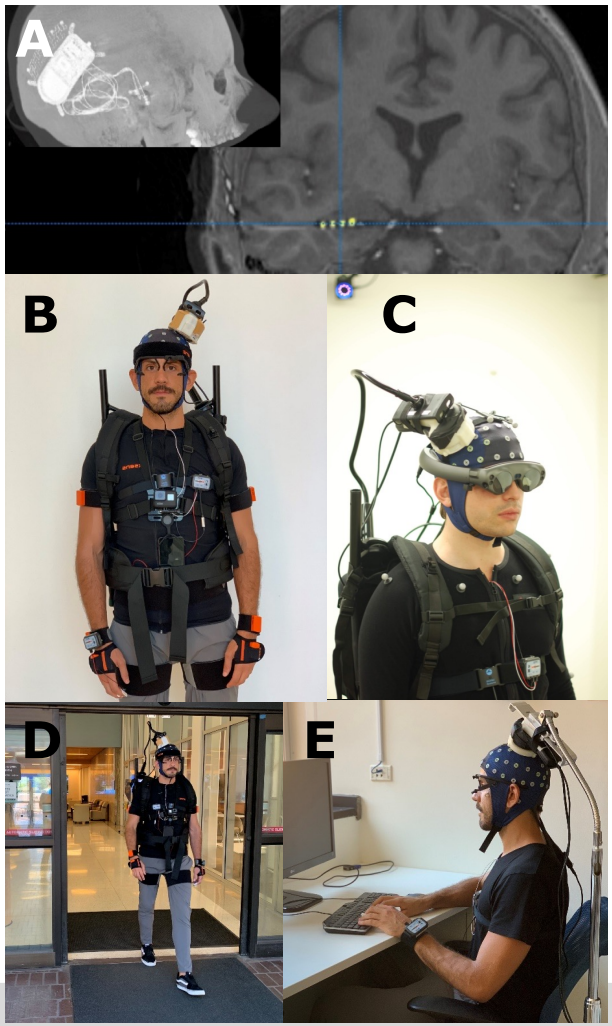
https://tinyurl.com/2cwxr6my

Project 1: Trustworthy IoT-in-the-loop Neuroscience

We developed a sensor suite that allows us to decode how humans ground episodic memories.

Active subprojects:

- Develop neurosymbolic architectures (XAI) for modeling the human sensory experience
- Secure, private, and resource-constrained inferences
- Safety modeling of IoT-in-the-loop neuroscience
- Stimulation through mixed reality



***NSF Neural Cognitive Systems #2124252**

RNS Neurostimulator

Wand Accessory

Neuropace Programmer Accessory

Neuropace Programmer

Battery Packs

Mobile Eye-Tracker

LED

- Eye-tracking data
- NTP Time
- Audio
- IMU

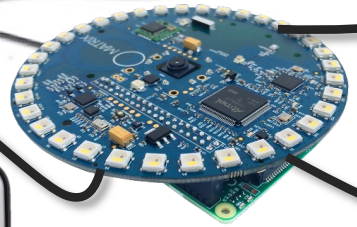
Psychophysiology

- EDA, ECG, resp
- IMU

1st Person Camera

NTP: Network Time Protocol

LED



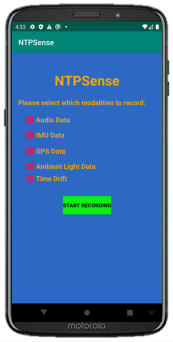
Single-Board Computer and 360° Audio

- NTP Time
- 360° Audio
- Sync to RNS, LED, audio

Movement Tracking

- IMUs
- Speed and Movement

GPS Phone



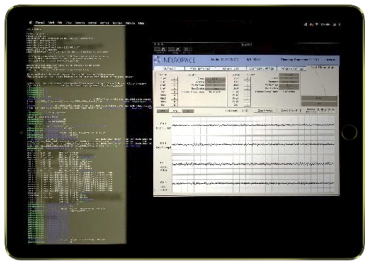
Sensors

- NTP Time
- GPS
- IMU
- Ambient Light

Participant

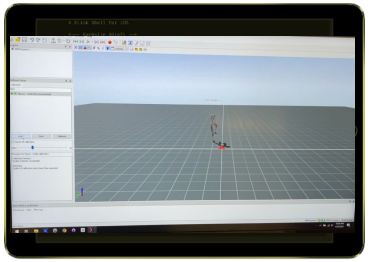
Clapperboard

360° Camera



Recording Monitor

LFP Recordings
Synchronization Log

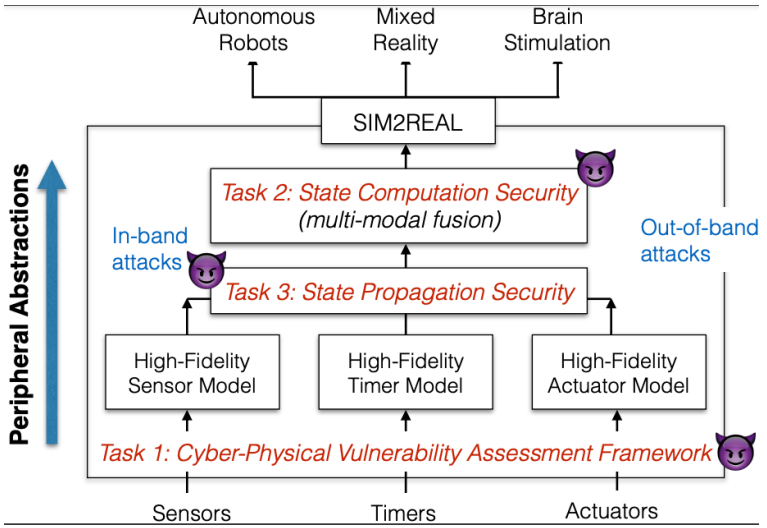


Xsens Monitor

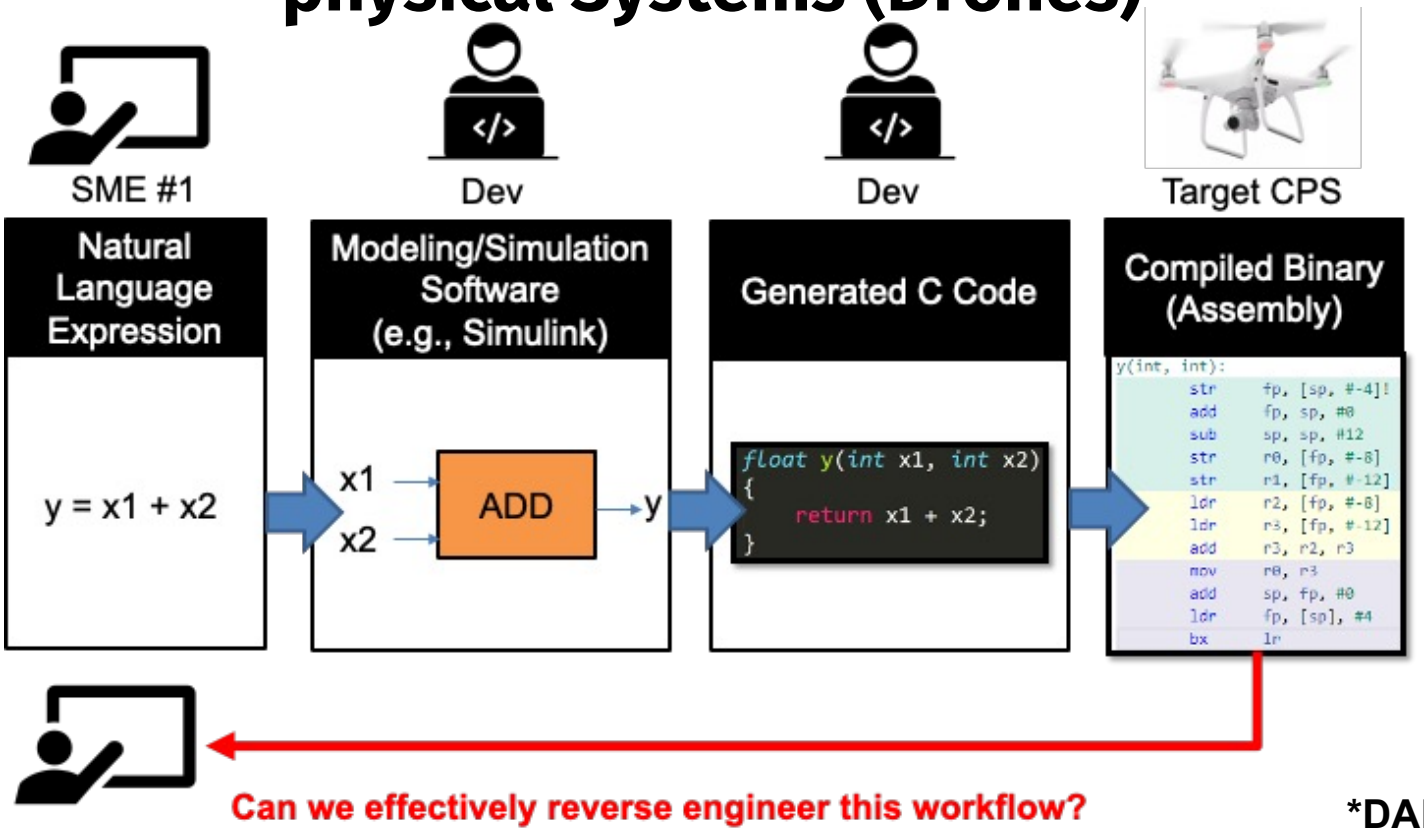
Project 2: Secure Peripheral Abstractions of Cyber-physical Systems

Active subprojects:

- Cyber-physical fuzzing framework
- Securing multi-modal fusion pipelines across safety-critical domains (e.g., robots, mixed reality, neuroscience)
- Securing state propagation across abstraction layers



Project 3: Semantic Reverse Engineering of Cyber-physical Systems (Drones)



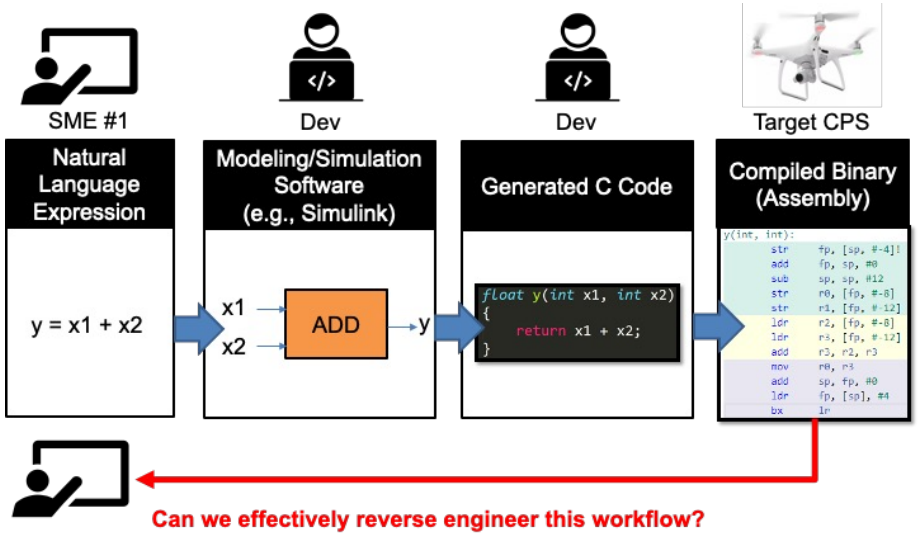
Can we effectively reverse engineer this workflow?

***DARPA AIE**

Project 3: Semantic Reverse Engineering of Cyber-physical Systems (Drones)

Active subprojects:

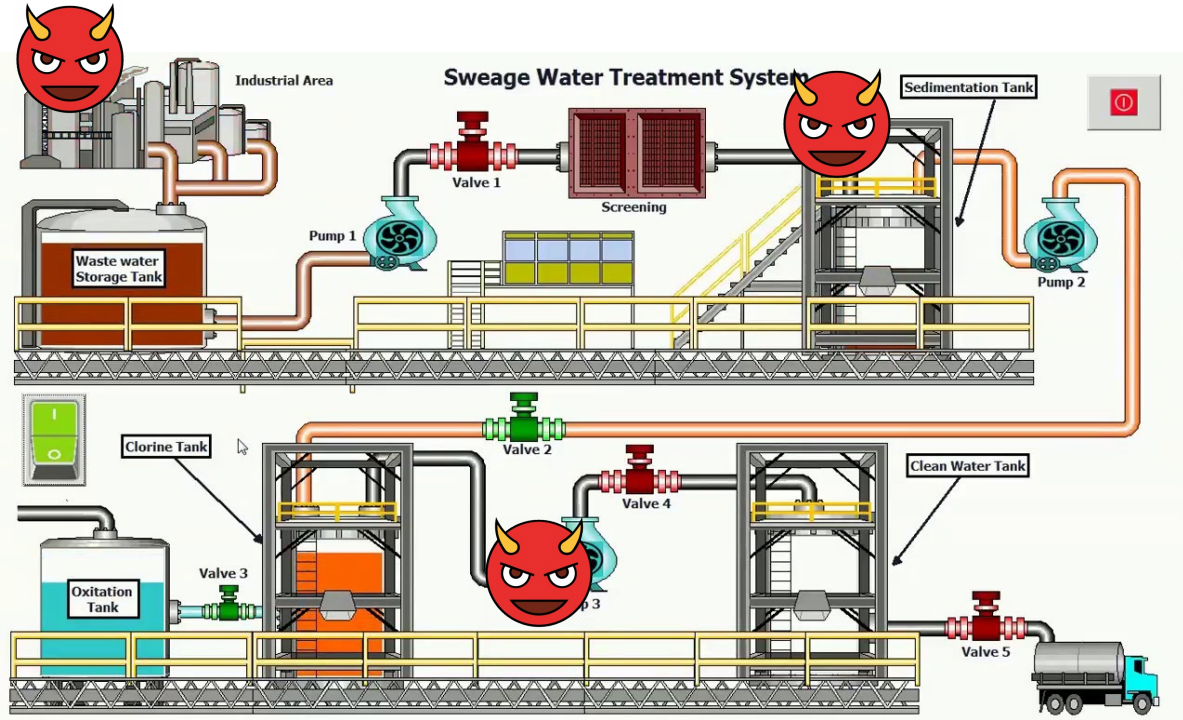
- Leveraging LLMs for reverse engineering tasks
- Modeling human factors in reverse engineering pipelines
- Building priors for automatic reverse engineering tasks
- Combing static/dynamic analysis with drone simulators



*DARPA AIE

Project 4: Formal Verification of Industrial Control Systems

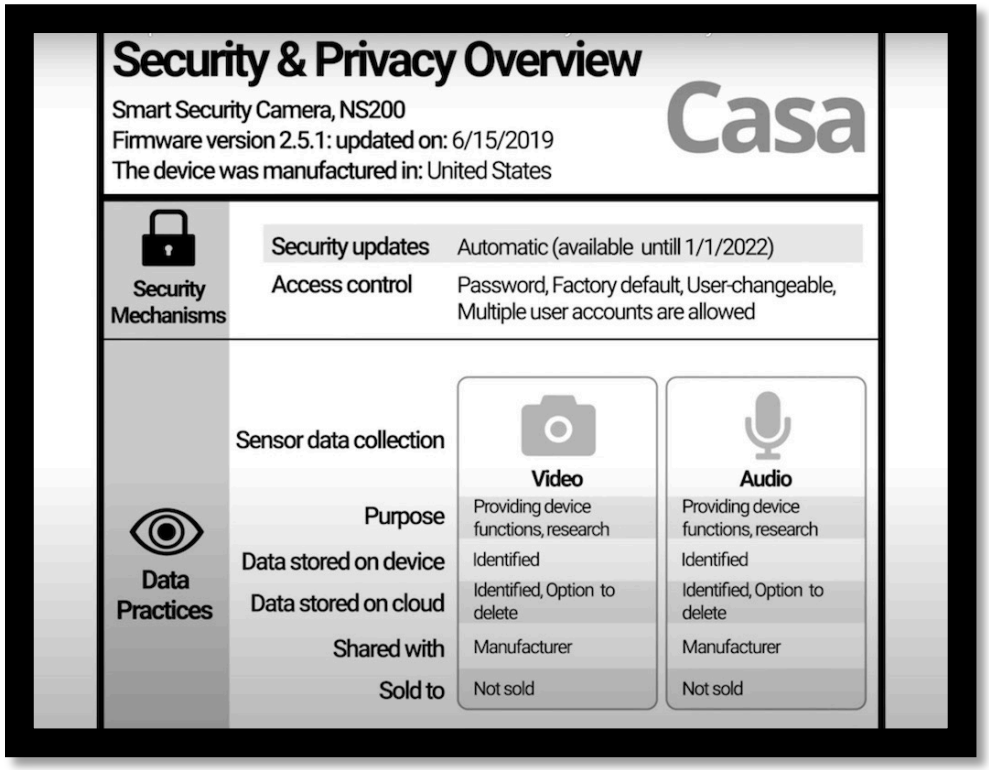
- Active subprojects:
  - Formally modeling and verifying software-based safety guarantees in the presence of adversaries
  - Modeling fidelity of cyber-physical simulators for cybersecurity experimentation
  - Analyzing time-synchronization standards in Industry 4.0



Project 5: Privacy Factors for Ubiquitous IoT Sensors

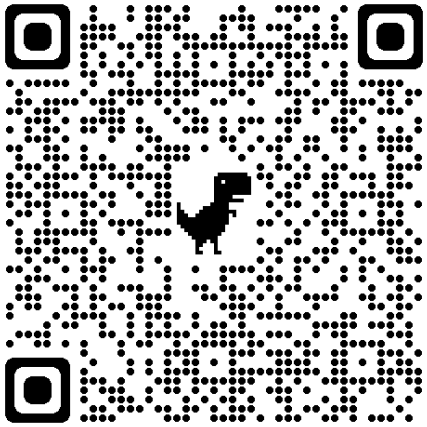
Active subprojects:

- Formal notions of privacy at the intersection of complex sensor embeddings
- Modeling human factors in light of privacy notions (and validating with user studies)



One last request

- Make sure to sign up for our course Piazza site!
- Fill out this survey on your background skills!
  - This will be used to adjust content as necessary, assign teams (if you can't find one), etc.




Questions?