Muslum Ozgur Ozmen

https://ozgurozmen.github.io/
@mozgurozmen

- Ph.D. Candidate @ Purdue CS
- Advisor: Dr. Z. Berkay Celik
- **Research Interests**
  - **Systems Security**
    - **IoT/CPS Security and Privacy**
  - **Applied Cryptography**

Career Highlights

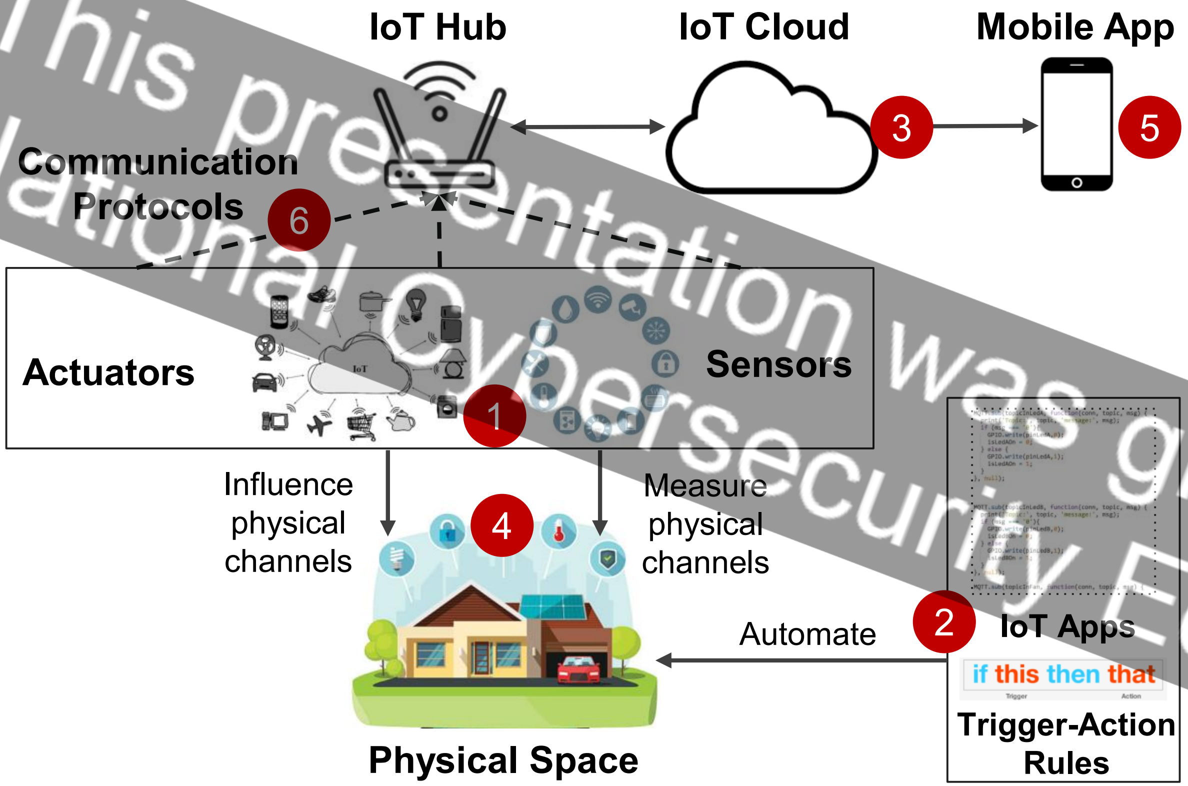
- **25 peer-reviewed publications**
  (IEEE S&P, USENIX Security, NDSS, ACM CCS, FC, IEEE TDSC…)
- **3 issued patents**
- **Internship with CPS Research Team at Toyota**

Research Agenda

🟥 First author

IoT Security and Privacy	AV/RV Security	Applied Crypto	Searchable Encryption	Human-Centered
CCS'22 🟥	NDSS'21	IEEE CNS'18 🟥	IEEE TDSC'18	Usenix Security'22
NDSS'23 🟥	IEEE S&P'22	CCS'18	IEEE ICC'18 🟥	NDSS'24
IEEE S&P'23 🟥	Usenix Security'23 (x2)	IEEE CNS'19 🟥	PoPets'19	
2 in Submission 🟥		FC'19 🟥		

Background



1 Software Vulnerabilities

2 App Interaction Threats

3 Access Control

4 Spoofing and Masking

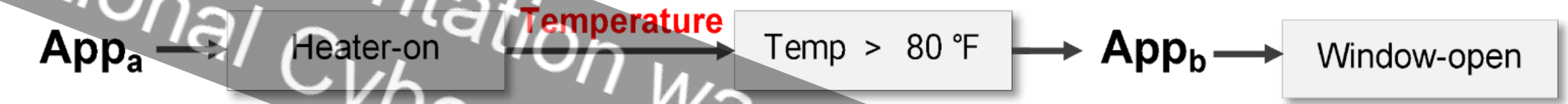
5 Mobile App Security

6 Privacy

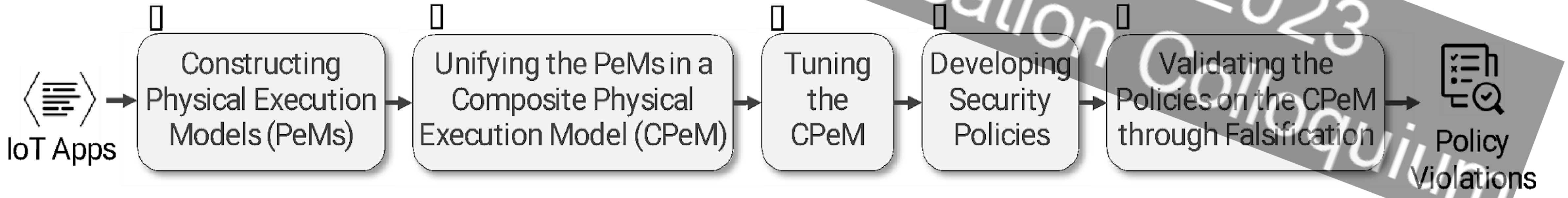
My research goal is to create a unified model for IoT environments and validate safety and security policies through the interplay of hybrid modeling and formal methods

IoTSeer [CCS'22]

- Problem: IoT apps interact over physical channels and cause safety and security issues in IoT environments.

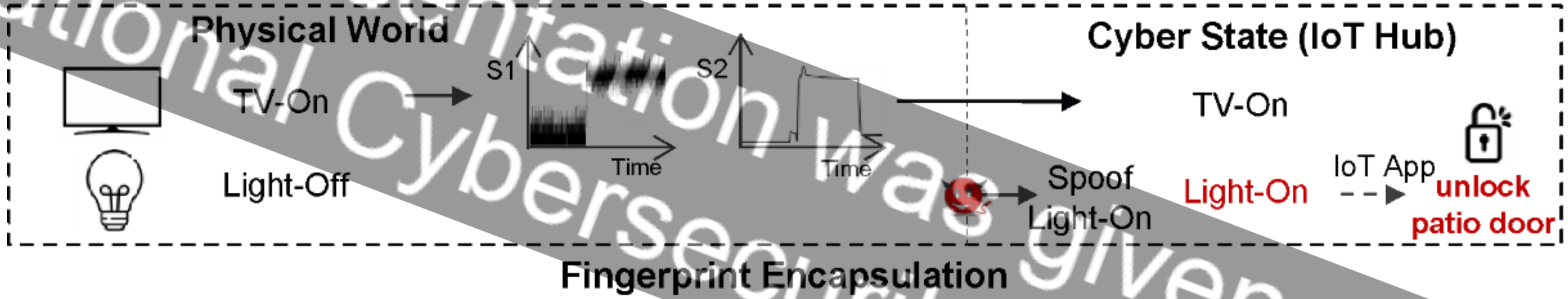


- IoTSeer builds the joint physical behavior of IoT apps in hybrid automata and validates security policies to discover physical interaction vulnerabilities


IoT Apps
Constructing Physical Execution Models (PeMs)
Unifying the PeMs in a Composite Physical Execution Model (CPeM)
Tuning the CPeM
Developing Security Policies
Validating the Policies on the CPeM through Falsification
Policy Violations

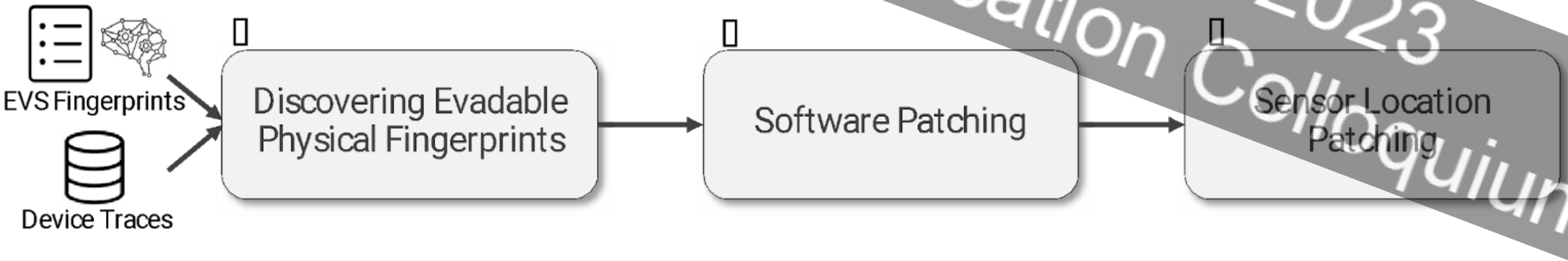
Evasion Attacks and Defenses [NDSS'23]

- Problem: Event Verification Systems (EVS) do not consider the complex physical relations between actuators and sensors, enabling evasion attacks



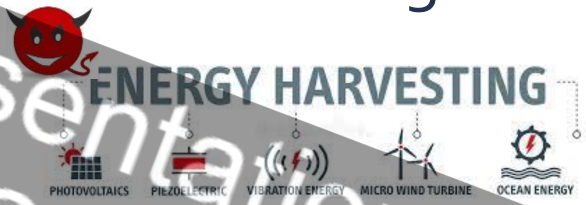
End States	
Physical	Cyber
TV-On	TV-On
Light-Off	Light-On

- We propose a system to make EVS robust against evasion attacks

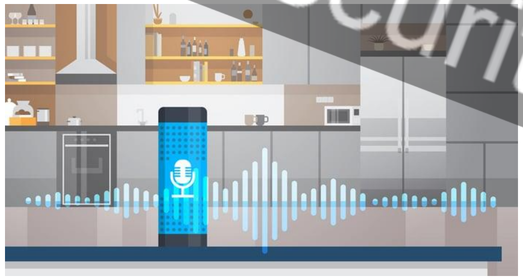


Ongoing and Future Work

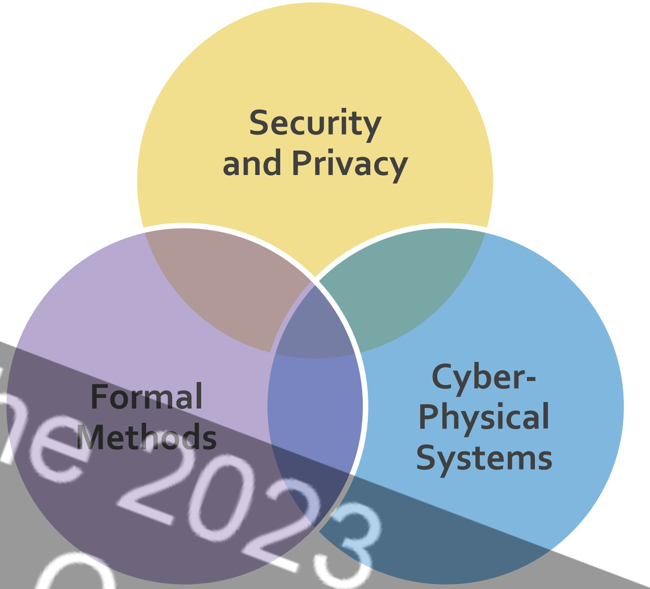
- Physical Side-Channel Attacks against Intermittent Devices



- Discovering Device Management Vulnerabilities in Voice Assistant Platforms



- Longer Term Research Plan
  - Automated Policy Generation for IoT and CPS
  - Forensics in IoT and CPS



Security and Privacy

Formal Methods

Cyber-Physical Systems

Thank you for listening!

https://ozgurozmen.github.io/

@mozgurozmen