Reliable Cyber-Physical Systems with Smartphone Cameras

Sun Bangjie
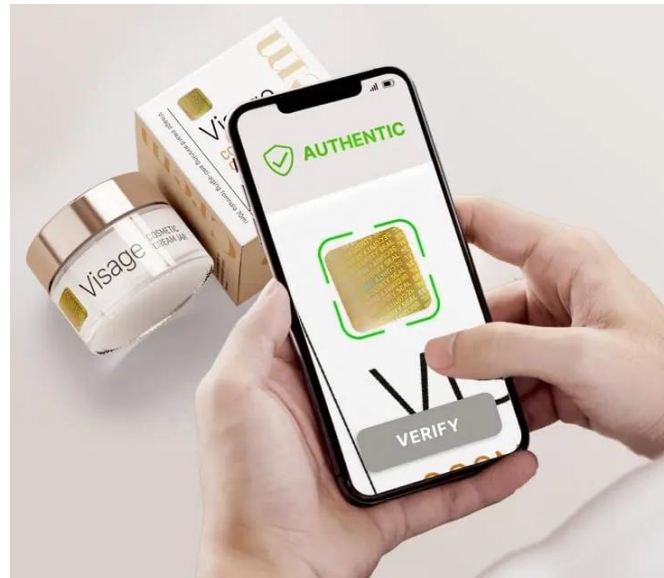
Advisor:

Prof. Chan Mun Choon

Introduction to Cyber-Physical Systems (CPS)
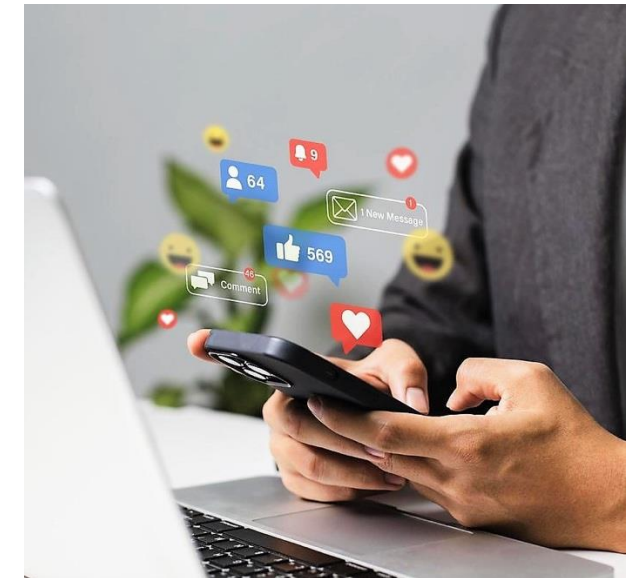
Cyber-physical systems (CPS) are **everywhere** and impact **everyday applications**.

Augmented Reality

Product Authentication

Information Sharing

Pitfalls of Current Vision-based CPS

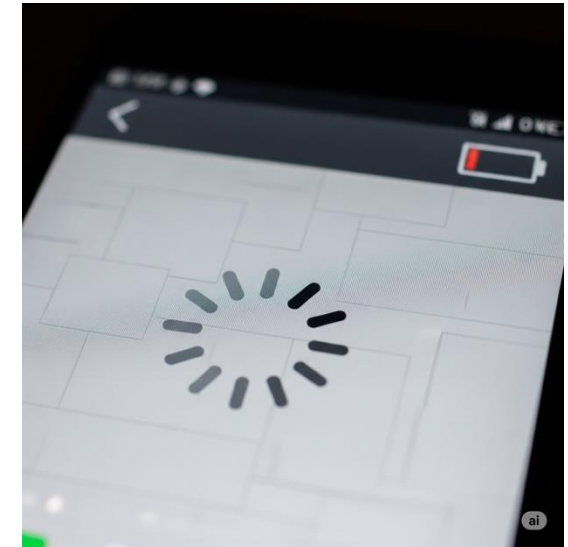Current vision-based CPS face **reliability** challenges.

Data Integrity
(e.g., manipulation and spoofing)

Data Uncertainty
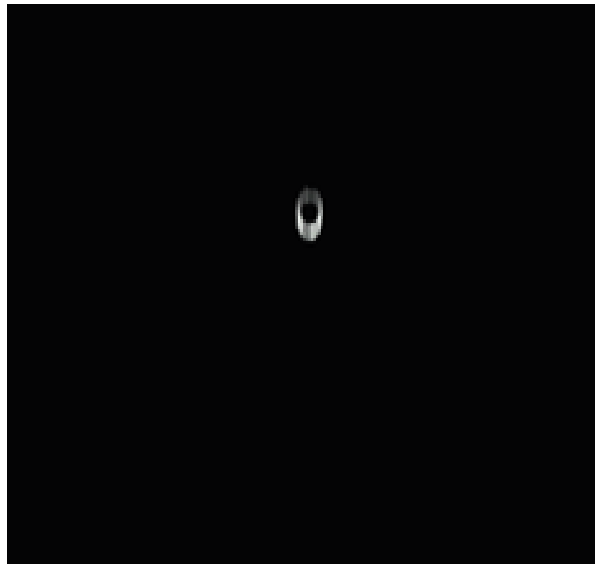(e.g., deceiving physical appearance)

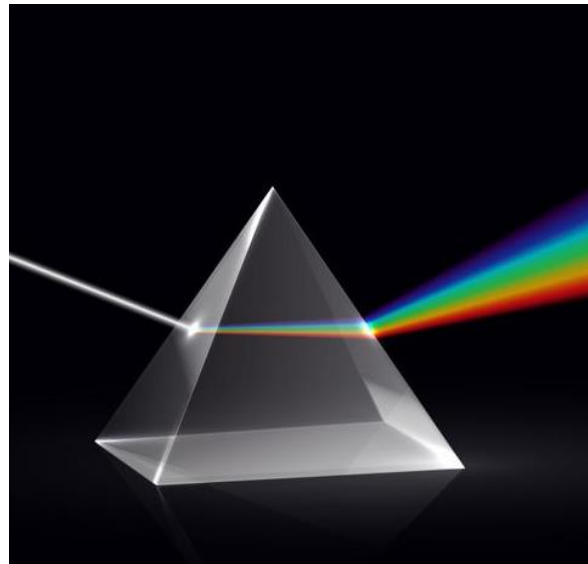**Computation**
(e.g., limited processing power)

Opportunity: Inherent Physical Characteristics

We can leverage the **unique**, **persistent** and **resistant** physical characteristics of real-world objects.
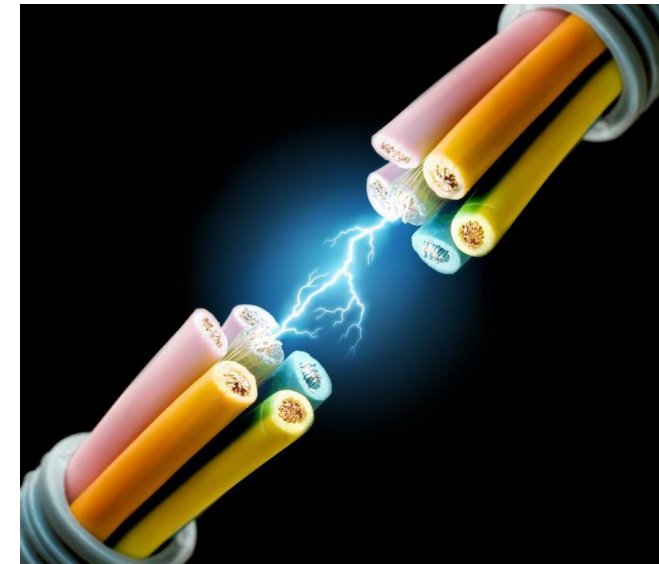
 # Physical Hash

Mechanical
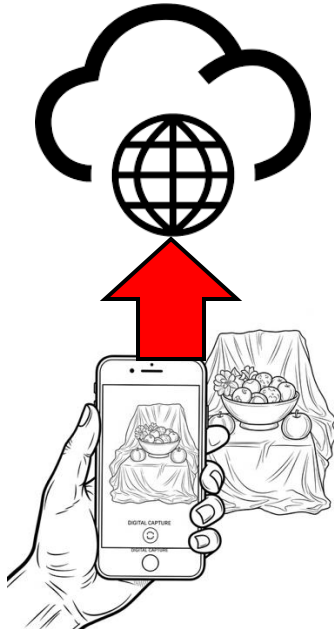
Optical

Electrical

Research Overview

My research is about building **reliable** vision-based CPS by utilizing **physical hash** to fortify **cyber-physical connections**

Research Overview

My research is about building **reliable** vision-based CPS by utilizing **physical hash** to fortify **cyber-physical connections**
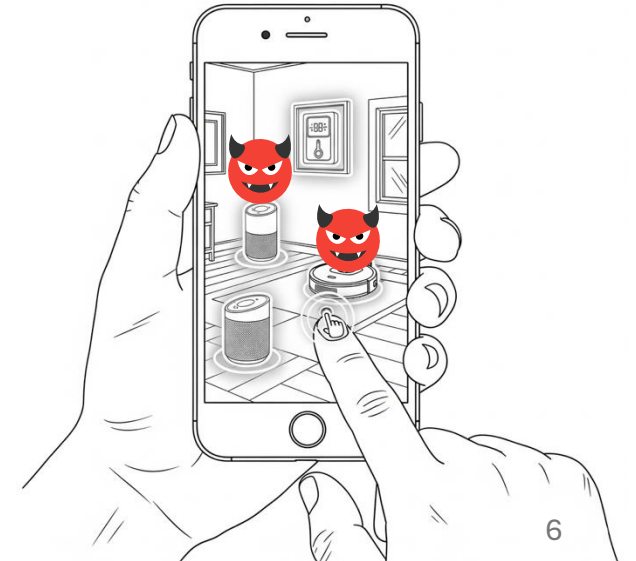
Physical Product Authentication

Digital Content Owner Attribution

Discovery of Vulnerability

Physical Product Authentication

Physical Product Authentication →
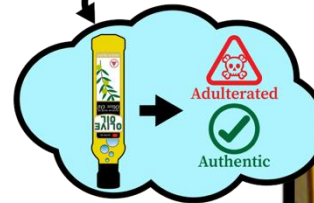
Best Poster

Liquid Form [MobiSys'22]

Textile Form [SenSys'23]

Best Paper

Powder Form [MobiSys'24]

Manufacturer's Cloud

Adulterated

Authentic

[MobiSys'22]

Liquid Testing

USER

SUPERMARKET

Digital Content Owner Attribution

Best Poster

Digital Content Owner Attribution

→ Photo Theft [MobiSys'25]

Generative AI [Submitted]

Digital Arts [Ongoing]

"BUT I FOUND IT ONLINE"

A Snapshot of Online Image Theft

Taken In a Flash

[MobiSys'25]

Instagram | Facebook | flickr | tumblr

CAMPrints

Sync

Charlie provides **reference photos** taken by his device

① **Coarse-Grained Detection**

Image database

② **Fine-Grained Detection**

Suspicious *Reference*

Notify Charlie

Discovery of Vulnerability

Discovery of Vulnerability → Deepfake Attack [USENIX Security'24]   Spy Cam Detection [SenSys'21]

Mallory

Foice

Bob's face image

Synthetic Voice Recordings × N

Attack Scenarios

Remote Attack   Verified!

Proximity Attack   *"Hey, Google! Open the door."*

Mallory Iterates through **all N** recordings

[USENIX Security'24]

Research Summary

Physical Product Authentication

Best Poster

Liquid Form [MobiSys'22]

Textile Form [SenSys'23]

Best Paper

Powder Form [MobiSys'24]

Digital Content Owner Attribution

Best Poster

Photo Theft [MobiSys'25]

Generative AI [Submitted]

Digital Arts [Ongoing]

Discovery of Vulnerability
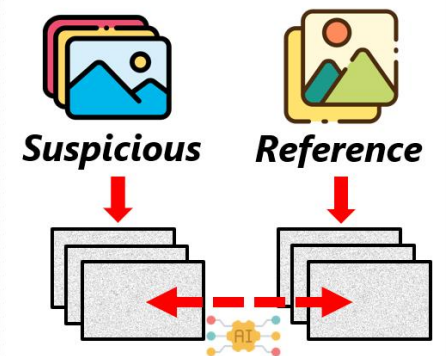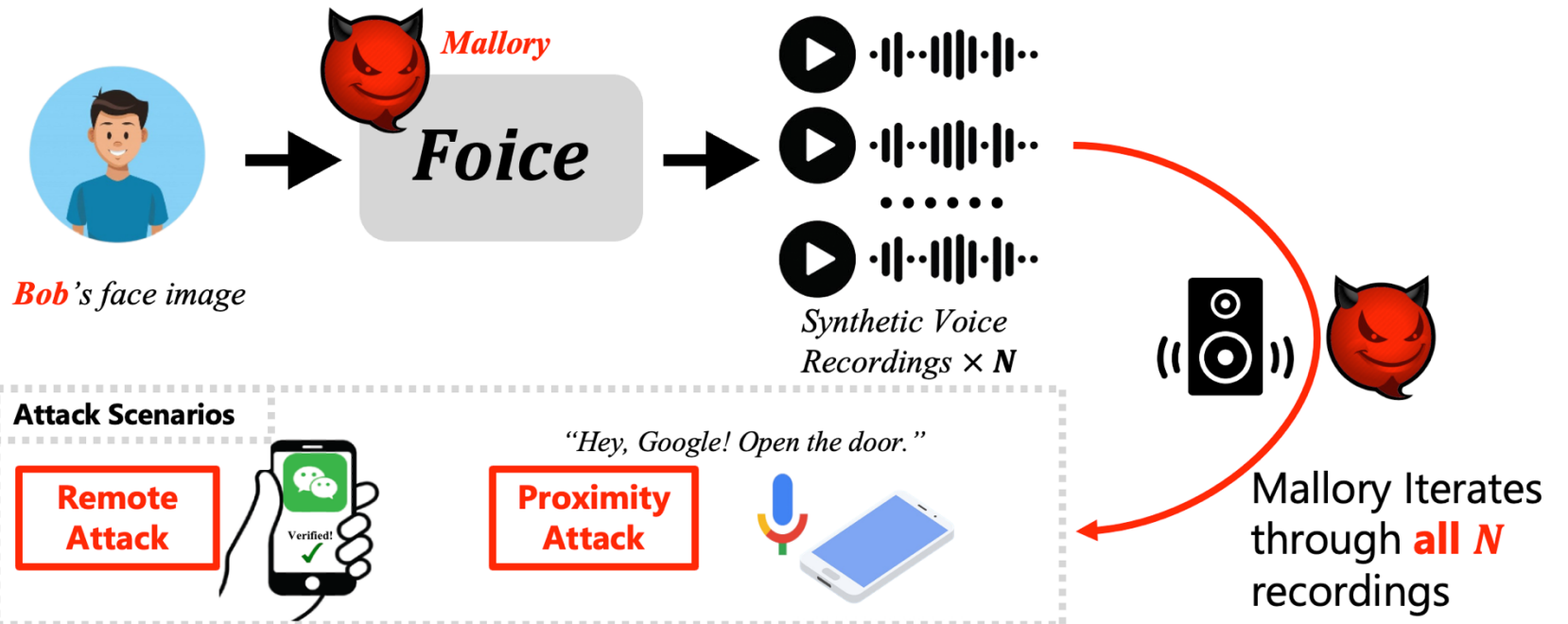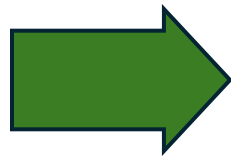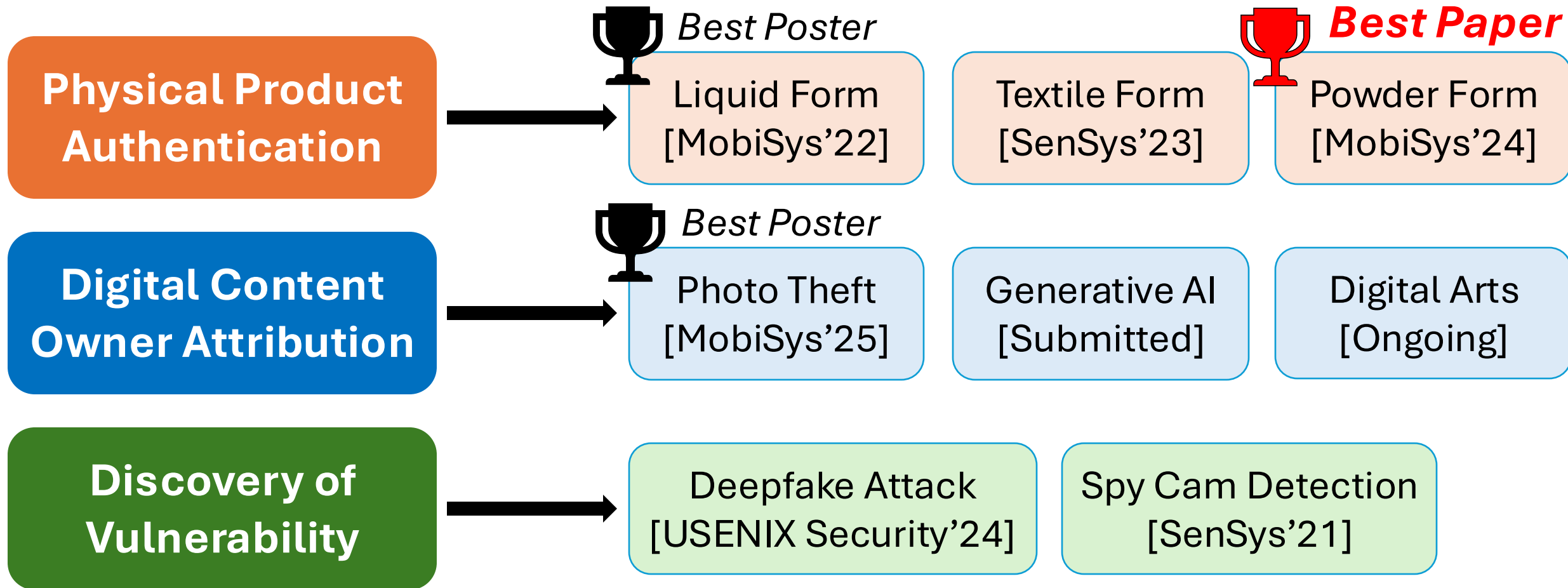
Deepfake Attack [USENIX Security'24]

Spy Cam Detection [SenSys'21]

Journey So Far

J.A.R.V.I.S. for Iron Man

Sense and connect with both worlds.

My research is making this a reality by enabling camera to **detect inherent physical characteristics**.

Thank you!

Scan me