

# Wireless Network Security and Privacy

## 无线网络安全及隐私

Xiaoyu Ji 冀晓宇

浙江大学电气工程学院

2025年9月23日

# About Me

Xiaoyu Ji 冀晓宇

2010: EE, BS, Zhejiang University

2015: CS, PhD, HKUST

2017-Now: Professor, ZJU

**Research interest:** IoT security, Embodied AI security, wireless and sensing security

**Homepage:** [www.xiaoyu.dev](http://www.xiaoyu.dev)

**Email:** [xji@zju.edu.cn](mailto:xji@zju.edu.cn)

**Office:** Rm. 325, Teaching Building #2

# About You?

## •Basic personal information

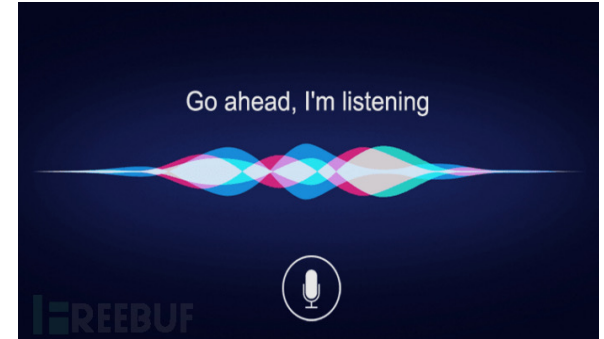
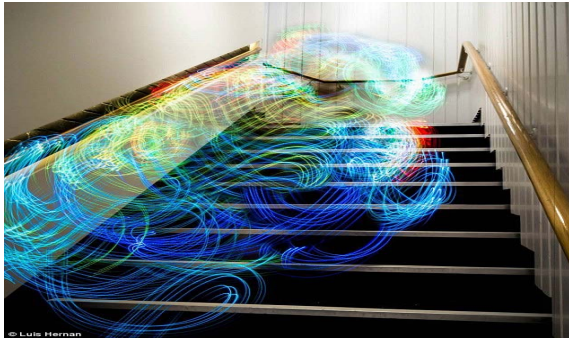
- Name
- MS/PhD/??
- Department
- Advisor
- Research Area
  - Interests
  - Experience

## •About this course and you

- Why do you take this course?
- What you expect to learn (or any goal)?
- What keywords run into your mind regarding wireless security?
- What specific problems or topics are you interested in?

# What is this course about?

- What is security?
- Is wireless secure, and why if not?
- What are the privacy issues in wireless networks?
- How to enhance the security of wireless networks?

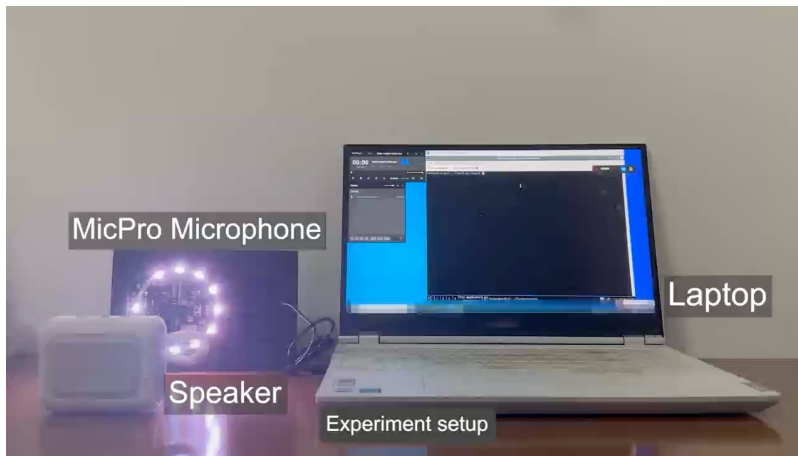


# Top X research problems in USSLAB

- Embodied AI security: attacks and defenses
- Sensor-oriented security and privacy problems
- Wireless signal for malware injection/ bug exploitation
- Wireless and electromagnetic signals to attack
  - GhosTouch series
  - Control manipulation
- Physical adversarial example
  - Laser to fool autonomous driving
  - Sound to fool autonomous driving
- Voiceprint/ASR/ASV security
  - Siri, 小度小度, 天猫精灵.....
- DolphinAttack and its defenses
- Nonspeaker as speaker to attack ASR
- GhosTouch, wired GhosTouch
- Liveness detection
- .....

# Sensor-oriented security and privacy

- MicPro (CCS'23) and CamPro (NDSS'24)
- Audio/Facial privacy protection on sensors



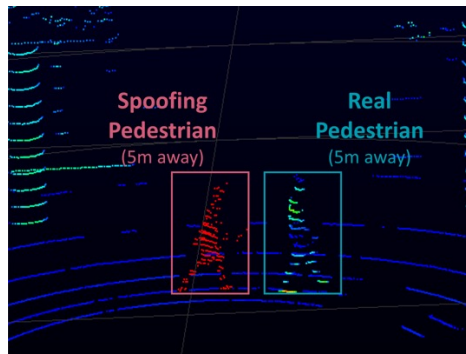
MicPro



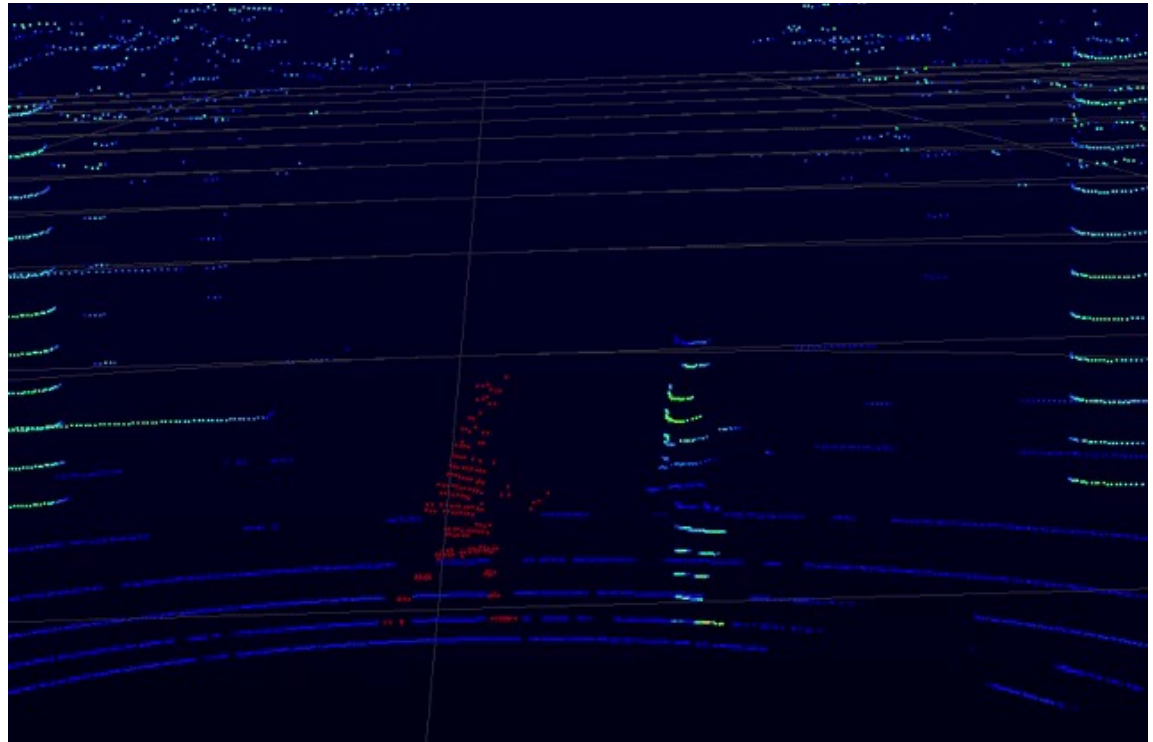
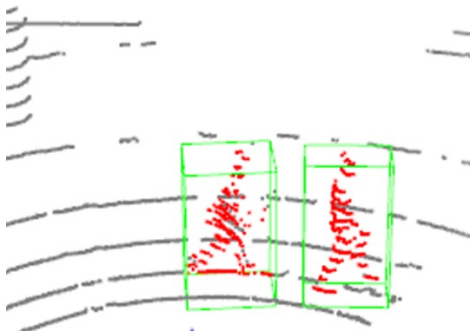
CamPro

# Physical adversarial example

- ADV-Lidar (IEEE SP'23)
- Laser to fool autonomous driving



Point cloud

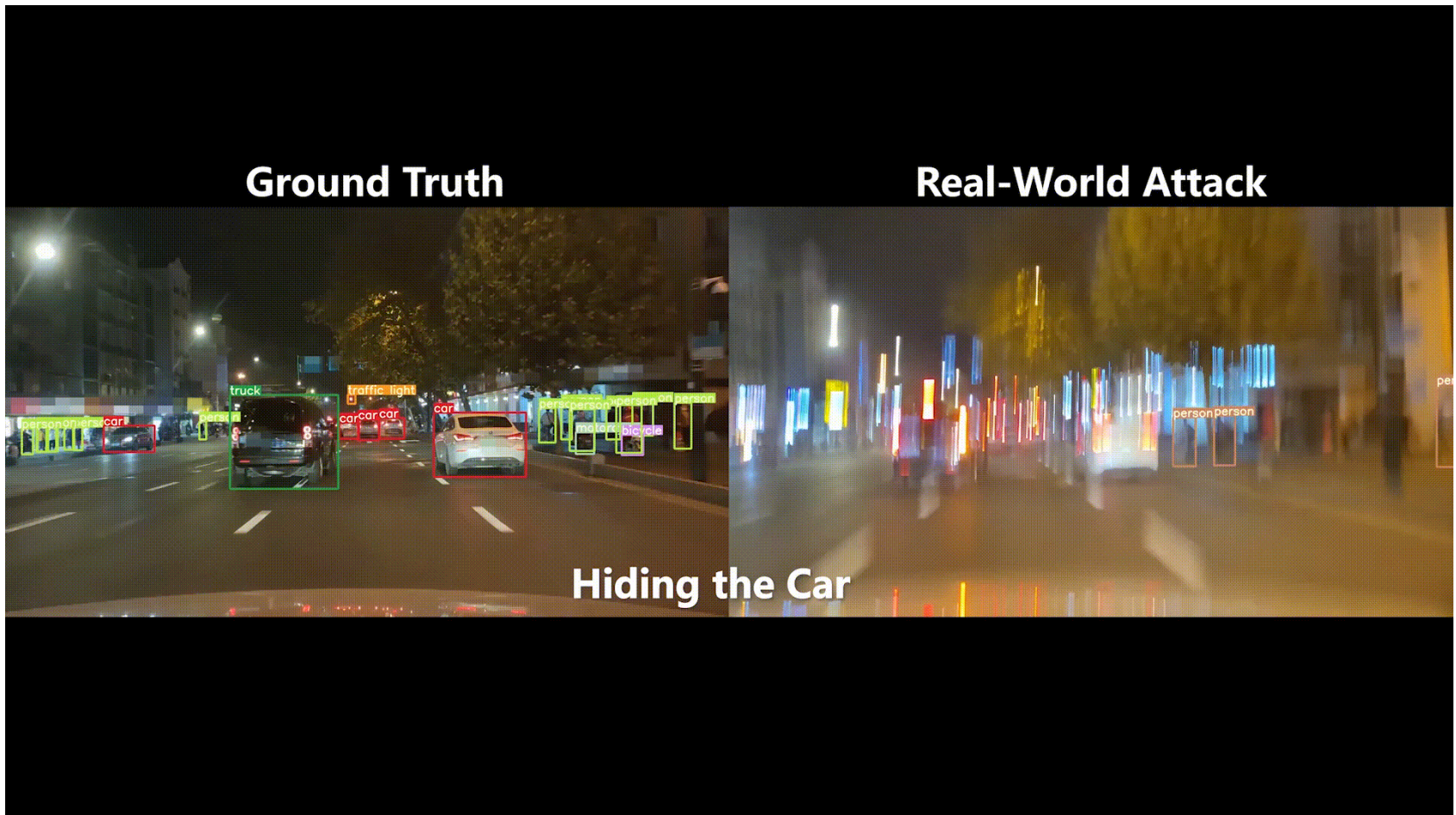


A spoofing "pedestrian" point cloud (left) and a benign pedestrian point cloud (right) are both detected by SECOND.



# Physical adversarial example

- Poltergeist (IEEE SP'21)
- Play sound to fool autonomous driving





# Voiceprint security

- PROLE Score (USENIX Security'22)
- How to measure voiceprint security
  - [www.ussslab.org/prolescore](http://www.ussslab.org/prolescore)

Voiceprint Security

## Comments

This is the demo homepage of the `PROLE score`.

`PROLE score` is used to evaluate the distinctiveness of speech content. Speaker verification using high-distinctiveness words can reduce the FAR and FRR, and improve the security of voiceprint.

## PROLE Score Tool

Our tool used to calculate the `PROLE score` is shown as below. You need to **select the ASV model** and **input words**, and the tool will return the `PROLE score` and give some recommendations of modifying the words to improve the security.

The functions of this tool are as follows:

1. Transform your input into phone sequence, filtering some digital numbers, special characters, and etc.
2. Calculate the `PROLE score` of your input.
3. Give the evaluation result of security level and some recommendations to improve the security.

**Speaker Verification Model**  
U-Level

**Input Word(s)/ Sentence**  
demo

Get Score

**Analysis & Recommendation**  
**Analysis:**  
The length of the input is short.  
The richness of the input is low.  
**Recommendation:**  
You'd better add 8 phones, including 6 different phones.

**Phone Sequence**  
demo  
**PROLE Score**  
7.9084  
**Security Level**  
Low!

# DolphinAttack

- **ACM CCS' 17 Best paper**
- **能力效果：**通过超声波注入无声的语音指令，可对手机语音助手进行各类指令操控，如打电话、访问恶意网页
- **作用对象：**具有语音助手的手机、平板、电脑、汽车等
- **作用距离：**20米（实验室原型机，距离可提升）

## 实际攻击演示（近距离概念展示）



通过超声波发生装置，产生无声语音指令，可以使苹果手机的Siri语音助手执行“拨打电话”的语音指令

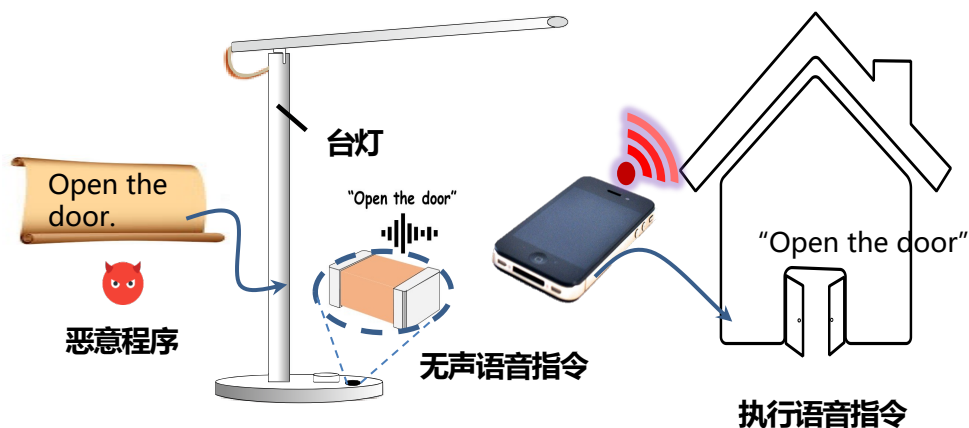
## 实际攻击演示（自制设备，20m攻击距离）



通过超声波攻击装置，在20m外发出无声语音指令，可以唤醒苹果手机的Siri语音助手并执行语音指令

# Nonspeaker attack ASR

- ACM CCS' 21
- **能力效果**：通过程序控制台灯等普通家用设备的电容发出超声波，可向智能设备的语音助手下达恶意命令，或实现隐蔽通信传输
- **作用对象**：普通家用设备、智能语音助手
- **作用距离**：10cm



基于电容发声的语音注入攻击

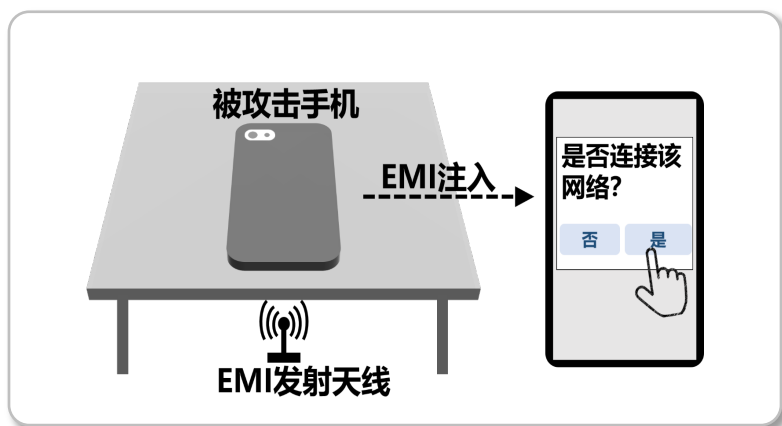


电容发声攻击演示

# GhosTouch

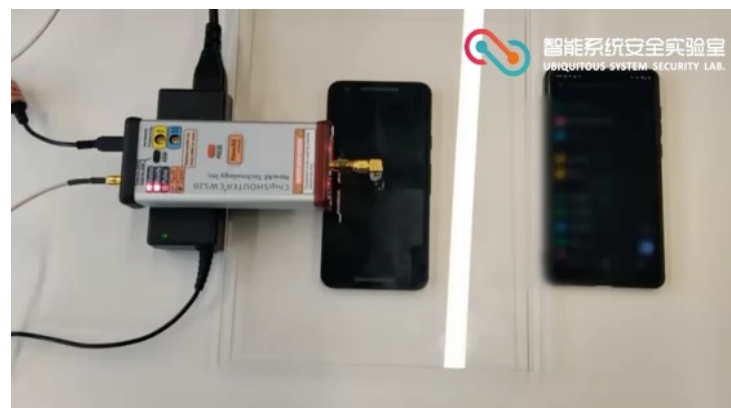
- USENIX Security' 22
- **能力效果**：通过电磁波操控目标手机，在无人接触屏幕的情况下实现对手机触摸屏的点击、滑动操作，可以接听电话、连接恶意蓝牙、接收恶意文件等。
- **作用对象**：有电容式触摸屏的手机、平板、电脑等
- **作用距离**：可跨桌面（攻击装置在桌下，被攻击手机在桌上）

攻击场景（连接恶意网络）



攻击装置藏在桌下，通过电磁波向桌上的手机屏幕注入虚假触摸点

实际攻击演示（接听电话）



左：攻击装置 中：被攻击手机 右：拨打电话手机  
通过电磁波产生虚假触摸点，实现电话接听。  
透明亚克力板模拟桌子

# Wired GhosTouch

## ■ IEEE S&P' 22

- **能力效果**：通过充电线操控目标手机，可在无人接触屏幕时操控手机、有人触摸时篡改触点或使触摸无响应
- **作用对象**：有电容式触摸屏的手机、平板、电脑等
- **作用距离**：取决于充电线长度

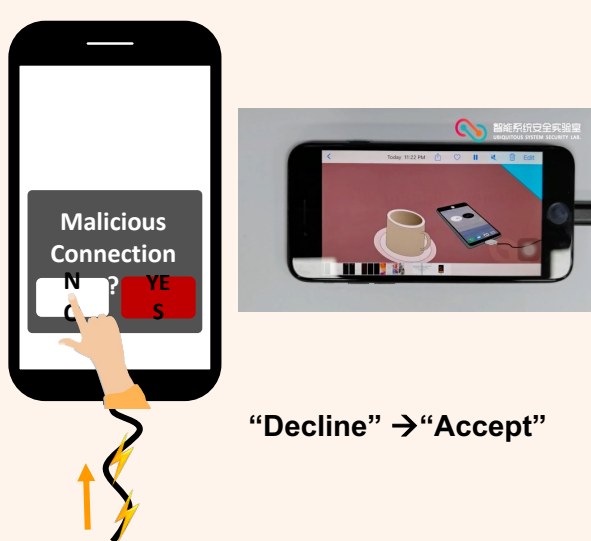
### ■ 注入攻击

用户无操作下注入鬼手触点



### ■ 篡改攻击

注入鬼手触点，篡改用户触点



### ■ 拒绝服务攻击

触摸屏无法接受用户触摸操作





# Other: Signal into control

- How to manipulate to attack the control of an UAV
- What is the rationale behind



# Course Goal

- **Understand the basic principles of wireless network security and privacy**
  - Wireless network basics
  - Security & privacy, especially related to wireless networks
- **Read and discuss interesting literature in the areas of wireless network security, such as:**
  - Wireless signal as an attack
  - Embodied AI attack and defenses
  - AI related security, e.g., adversarial ML
  - Software and protocol security
  - Other new trends, e.g., 5/6G security
- **Understand and get a sense on how to do research**
  - How to determine what is important
  - How to organize a research paper
  - How to *sell* your idea
  - How to present your work?



# Administrative

## Course information:

- Syllabus: publish after each course
- Reading references: TBD in next course
- **Course web:** <http://www.usslab.org/courses/wnsp.html>

## How to reach me:

- **Email:** xji@zju.edu.cn
- **Office:** Teaching Building #2, Rm 325
- **TA:** Yu Wang (王禹)

## Recommended reference book:

- 《物联网安全》，徐文渊、冀晓宇等
- Computer Networking: A Top-Down Approach
- “Cryptography and Network Security” by William Stallings
- William Stallings[美]著. 刘玉珍,王丽娜,傅建明等译, 《密码编码学与网络安全—原理与实践》(第六版), 电子工业出版社, 2004

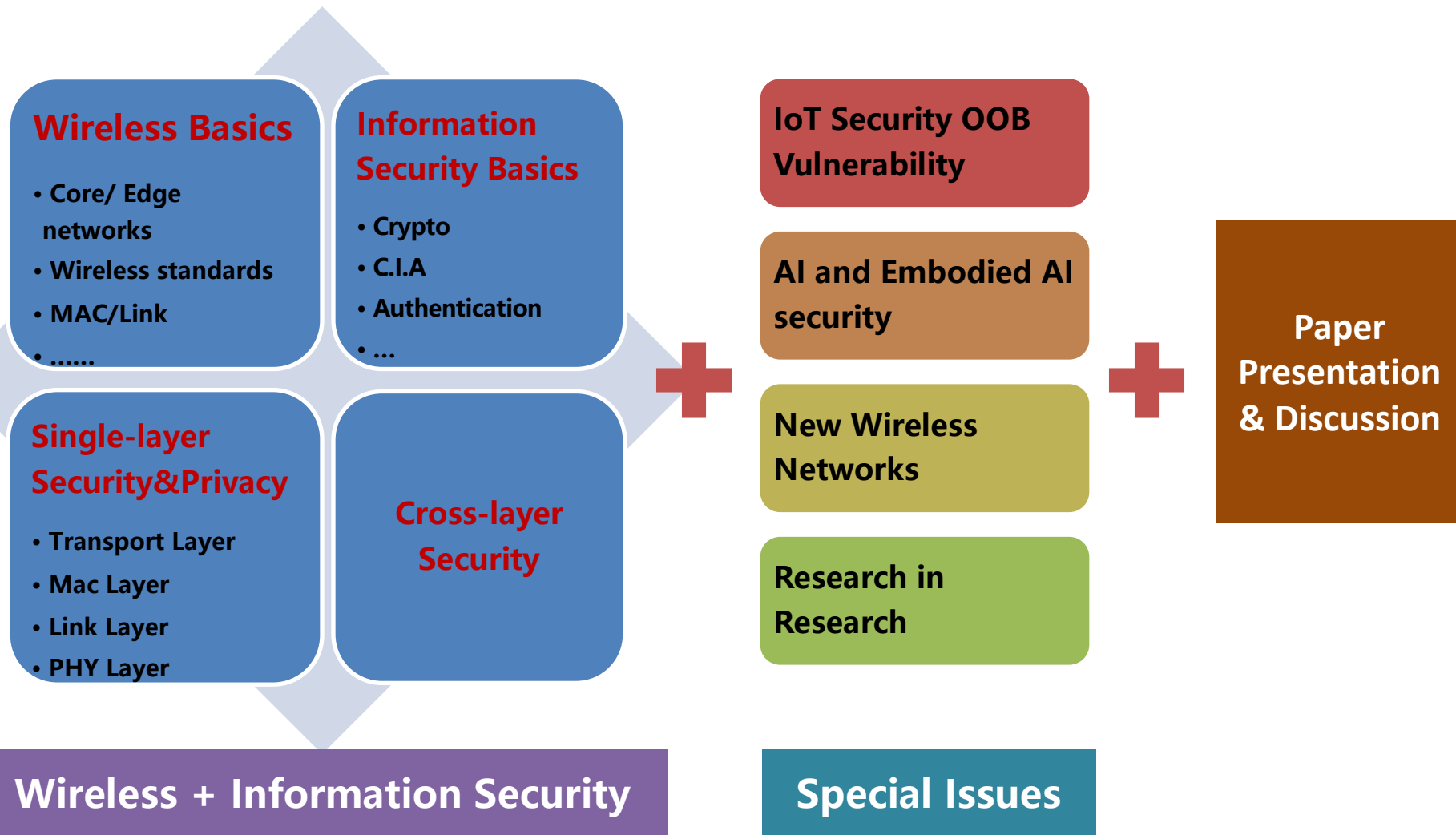
# Pre-requisites

- Computer networks
- Basic programming skill, e.g., Python/C/C++
- Basic knowledge of wireless
- Strong motivation
- Curiosity

# Tentative Topics

- **Wireless networks [1 course]**
  - Wireless concepts
  - Wireless standards, e.g., IEEE WiFi/802.11
  - Mobile networks: smartphones
  - Narrow-band IoT (NB-IoT), 5G
- **Information Security basics [1 course]**
  - Concept of cryptograph
  - Classical and modern cryptograph mechanisms
  - IoT authentication, hash, etc.
- **Wireless Security & Privacy [3 course]**
  - Single layer security & privacy
  - Cross-layer security & privacy
  - Location based security & privacy
- **Special Issues [2 course]**
  - IoT Security OOB Vulnerability
  - AI and Embodied AI Security
  - Security and privacy in new wireless networks
  - Research in research (\*)

# Course Organization



# Course Organization

- Group task

# Course Organization - Presentation

- Each student presents 1 paper: from top-tier security conferences
- Paper source: ACM CCS/Usenix Security/ IEEE S&P, NDSS, and I will recommend a list of recent papers
- Will run like a seminar
  - My introduction about the topic
  - Your presentation of papers of that topic
  - Discussion from all students
- Auditors are expected to read papers and participate
- Papers are divided into several sessions according to its topics

# Grading

- No exam!
- Grading based on:
  - 50% class discussions and participation
  - 50% presentations
- Your Best Strategy
  - Come to every lecture
  - Read and summarize papers that will be presented
  - Participate in the discussion during class!
  - Enjoy the fun!