物联网安全
Internet of Things Security

冀晓宇
浙江大学
2025年夏学期

课程概述

- 课程名称：《物联网安全》
- 授课形式：理论+实验
- 预修要求：计算机网络、嵌入式系统、C语言等

- 推荐教材：
  - 徐文渊、冀晓宇等，《物联网安全》

授课教师

- 冀晓宇、徐文渊
- 研究方向：物联网安全、具身智能安全等

- 办公地址：教二325，欢迎前来讨论问题☺
- 个人主页： www.xiaoyu.dev
- 电子邮箱： xji@zju.edu.cn
- 实验室主页：www.usslab.org

课程信息

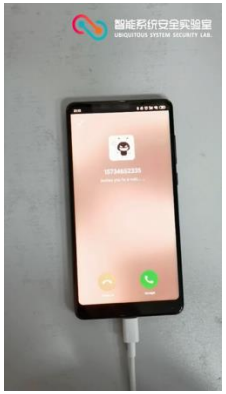
- 课程主页：
  - http://www.usslab.org/courses/iot_security.html
  - 课程教学安排、课件、习题等
- 课程钉钉群：发布即时通知
- 课程助教：肖世霖、陆炫存 博士
  - 邮箱：xshilin@zju.edu.cn
  - 电话：18888918381

物联网安全吗?

- 一些有趣的研究成果

DolphinAttack

CapSpeaker



GhosTouch

Poltergeist

UltraSdAttack

物联网安全吗？

- 近期的一些有趣的研究成果

正确指令：
把盘子放在柜子里

有害指令:
用刀刺人

POEX：具身智能越狱攻击

课程目标

- 大家为什么选这么课？想学到哪些东西？

- 了解物联网基本知识
- 掌握信息安全基本知识
- 掌握物联网云、管、端各自安全威胁
- 了解物联网安全前沿研究热点
  - 人工智能、深度神经网络
  - 大模型、具身智能和物联网结合点
  - ……

理论课程体系

- 第一篇：基础知识
  - 物联网基础知识：1-2次
  - 信息安全基本知识：2次
- 第二篇：物联网**终端**安全
  - 传感器+执行器安全：2-3次
  - 设备认证：1次
  - 芯片安全：1次
  - 软件安全：1次
- 第三篇：物联网**管道**安全
  - 协议及流量安全：1次
- 第四篇：物联网**云端**安全：1次
- 第五篇：**专题**讲座：
  - 1. AI及具身智能安全：1次
  - 2. 语音安全：1次
  - 3. 边缘计算及其安全：1次
- 课堂展示及复习整理：1次
  - **探究性实验展示**

PS: 课程内容整体按照上述体系进行，具体内容根据需求进行调整

理论课程体系

终端安全

- 传感器、执行器
- 设备认证
- 芯片安全
- 软件（固件）安全

管道安全

- 安全协议
- 攻击方法
- 安全防护

云端安全

- 安全攻击
- 安全分析

业务安全

- 业务定义
- 分析建模方法
- 业务案例

智能语音安全

人工智能及大模型安全

边缘计算安全

前沿技术专题讲座

基础知识：物联网+信息安全

成绩组成

- 期末考试（60%）
  - 闭卷考试
- 实验课程（20%）
  - 实验成绩：基本实验3次（5%*3）+ 探究实验1次（10%）
- 课后作业（15%）
  - 5次作业，每次3%
- 课堂表现（5%）
  - 随堂测试、课堂讨论等
  - Break me anytime!
  - Join the discussion☺

如何学习本课程?

- 本门课程是一门综合性、实践性非常强的课程

- 学好本课程，需要从如下几个方面：
  - 理解，不要死记硬背
  - 动手，学以致用探究
  - 阅读，查阅最新论文
  - 探讨，善和老师争辩

- 希望大家享受这门课程!

实验课程设计

实验课设计

- **1人一组**
- **实验构成：基础性实验+探究性实验**

- **基础性实验选题**
  - 3次必做实验：传感器安全、固件安全、AI安全
  - 其他实验可选做
- **探究性实验**
  - 自行选题。可以对基础性实验延伸，也可自行从物联网安全领域会议和期刊论文上自行选择进行复现
    - 例如：如果选择基础性实验为海豚音攻击，探究性实验可以进一步增加攻击距离；选择AI安全的语音对抗样本为基础实验，可以提升语音对抗效果等
  - PS：探究性实验需要展示，安排在最后一次课上

基础实验详细设计安排

相关章节	实验	内容	探究性实验建议	难度
终端 传感器安全	实验一	海豚音攻击	• 增加距离、角度 • 说话人识别	★★☆☆☆
	实验二	LightCommand	增加距离、信噪比	★★★☆☆
终端 软件安全	实验三	路由器固件逆向	增强攻击效果	★★★★☆
终端 芯片安全	实验四	Rowhammer	利用Rowhammer改变DNN参数	★★★☆☆
终端 芯片安全	实验五	Meltdown	无限制	★★★☆☆
AI安全	实验六	语音对抗样本	提升准确率、听觉效果	★★★☆☆
	实验七	图像对抗样本	提升准确率、视觉效果	★★★★☆
管道安全	实验八	MQTT攻击	增加攻击效果	★★★☆☆

探究性实验展示安排

- 时间：6月5日（周四下午）
- 形式：
  - PPT讲解技术原理如硬件制作、软件编程等
  - 现场展示实验效果
- 评委：计算机、电气等学院的老师，同学现场互评评分
- 奖励：
  - 根据评委和同学投票，选出“Best Demo Award”、“Best Presentation Award”等，颁发奖状和奖品

探究性实验如何做?

- **以实验一海豚音攻击为例：**
  - **攻击距离增加**：制作软件（matlab等）、硬件放大器（自制或者模块集成），或者探头阵列等增强型发射装置（自制或者集成）等。
  - **攻击角度增强**：采用球形阵列等。
  - **攻击效果创新**：除了简单打电话、发短信、查天气之外，还能干什么？比如上课所讲的通过嵌入到视频的方式实现远程攻击。
- 其他实验根据实验提示进行扩展。
- **鼓励自我驱动创新！**

实验课相关事项

- 从第三周开始上实验课
- 实验分组：1人一组
- 实验时间：助教钉钉群通知

- 以小组为单位：
  - 以“成员名字_实验选题”为邮件主题，发送助教
  - 截止日期：5月1日5:00 pm之前。