2024年
《物联网安全与隐私保护》课程
大作业要求

- 任课教师：王秀华 周　威
- 课　　时：24 学时
- 学　　分：1.5学分

成绩构成

- 平时成绩（50%）
  - 签到（10%）4次
  - 课上和课下作业（微助教提交）（40%）
    - 物联网密码学应用（20%）
    - 物联网系统安全（20%）
- 课程报告（50%）
  - 实验报告/论文阅读报告二选一

论文阅读报告要求

- 论文选择
  - 物联网密码学/物联网系统安全两个方向选**其一**
  - 相关顶级会议或期刊上指定的前沿科技论文（可选列表后续发布）
  - 同一篇论文选择人数**不能超过2个**
  - **至少2500字 少一百字扣2分**
- 报告撰写要求
  - 具体要求：中文撰写，报告结构清晰，逻辑通顺，中文表达流畅。
  - 使用latex撰写（推荐使用overleaf的免费服务），**不适用此格式扣30%的分数**
  - https://www.overleaf.com/learn/latex/Chinese
  - 报名名称：**姓名-班级-学号-所选论文编号**
  - 具体要求见后（每一个大点为一个\section，每一小问是\subsection)
- 报告提交
  - 电子版：微助教提交**截止时间 5月12号 23点59分**
  - 纸质版：以班级为单位统一提交到指定教室（届时通知）

论文阅读报告要求（前18序号）

- 物联网密码学应用类：
  - 1、论文的研究背景及主要贡献。
  - 2、系统架构介绍。
  - 3、当前研究现状是什么（需要引用相应的参考文献）？
  - 4、论文所需的先验知识，或所需相关工具的简要介绍。
  - 5、论文提出方案的具体介绍，需说明方案为何可以解决论文提出的问题？
  - 6、论文的实验分析，包括实验环景搭建、实验数据来源、实验参数设置及实验对比结果等。
  - 7、论文阅读心得。

论文阅读报告要求（后18序号）

- 检查工具类：
  - 1. 论文目标检测的是安全问题是什么以及安全假设(Thread Model理解翻译)?
  - 2. 论文提出的工具或者方法相比于之前的工具关键优势是什么？（多个指标对比类别需要列表翻译） （需要引用相应的参考文献）
  - 3. 工具设计的主要技术难点以及主要方法概述 （插入架构图的请截图或重画）
  - 4. 工具实验对比结果有哪些项?**每项**实验设计的目的是什么？测试用例来自哪里？**每项**实验如果是对比其他工具的实验说明最好和最差是哪一个测试用例？原因是什么？如果是自身工具指标测试，说明指标中表现最好和最差是哪一测试用例？原因是什么？
  - 5. 你自己认为该工具存在什么问题？
  - 6.论文阅读心得

论文阅读报告要求（后18序号）

- 每一大点是一个section小问是subsection
- 攻击类别：
  - 1. 论文目标是针对什么具体场景和协议中什么安全问题进行分析和其他工作的区别是什么（需要引用相应的参考文献）？
  - 2. 论文发现的设计缺陷或漏洞有哪些？成因分别是什么？(列表总结)
  - 3. 论文利用发现的问题设计了哪些攻击？每种攻击的场景、假设、步骤和危害结果分别是什么？（论文中有图的需插入截图或者是重画）
  - 4. 论文实验针对哪些对象进行了测试？攻击测试项有哪些？**每项攻击测试**设计的目的是什么？测试结果中存在某些对象未达成论文的攻击测试的原因是什么？
  - 5.论文针对这些攻击提出了哪些缓解措施？（可自己补充）
  - 6.论文阅读心得

论文阅读报告要求（后18序号）

- 每一大点是一个section小问是subsection
- 防御与加固工具类：
  - 1. 论文目标抵御或修复的是安全问题是什么以及安全假设(Thread Model理解翻译)?
  - 2. 论文提出的工具或者方法相比于之前的工具的优势在哪里?（多个指标对比类别需要列表翻译）（需要引用相应的参考文献）
  - 3. 工具设计的主要技术难点以及主要方法概述（插入架构图的请截图或重画）
  - 4. 工具实验对比结果有哪些项?**每项**实验设计的目的是什么？测试用例来自哪里？**每项**实验如果是对比其他工具的实验说明最好和最差是哪一个测试用例？原因是什么？如果是自身工具指标测试，说明指标中表现最好和最差是哪一测试用例？原因是什么？
  - 5. 你自己认为该工具存在什么问题？
  - 6.论文阅读心得

论文阅读报告要求（后18序号）

- 物联网隐私泄露分析类：
  - 1. 论文目标检测或调研的隐私问题是哪些？具体调研的对象有哪些？和其他相关隐私工作的重点区别是什么？（需要引用相应的参考文献）
  - 2. 大规模调研所使用的具体方法和原理是什么？
  - 3. 调研每项的结果是什么？背后的原因有是什么？（可自己补充）
  - 4.论文中给出的建议有哪些？（可自己补充）
  - 5. 论文心得

实验报告要求

- 实验内容
  - 物联网云平台与协议和设备固件安全分析二个实验选题任选其一
  - 同一个选题选择人数不超过6人
- 报告提交
  - 电子版微助教提交 **截止时间 5月12号 23点59分**
  - 纸质版：以班级为单位统一提交到指定教室（届时通知）
- **实验中发现的未知安全问题会帮助大家申请获得CNVD或CVE编号甚至是社区与厂商的官方致谢**

物联网应用与平台实验（需两个同学配合完成）

- 阿里云IoT平台服务试用
  - https://free.aliyun.com/?product=1411&crowd=personal
  - 免费试用1个月
- 按照教程安装环境
  - 构建直连物联网设备即可
    - **注意设备名称为自己的学号**
  - 消息协议使用MQTT类型
  - 设备起码要具备上报和接收云端指令两种功能
  - 利用MQTT工具测试课上讲的MQTT四种漏洞缺陷
    - 两个同学互相作为受害者和攻击者进行测试
  - 扩展测试MQTTactic
  - 自定义测试其他授权与认证问题

- 实验报告撰写要求
  - 1. 设备的云服务构建过程
    - 设备创建截图 包含学号的设备名称
  - 2. 正常设备通信时候的发送与接收的模拟器动态消息输出截图完整消息内容包含设备名称截图
  - 3. 每种攻击的具体设置与具体的攻击测试步骤以及消息截图包含学号
  - 4. 实验心得

物联网固件开发与逆向分析实验

- 0.查阅CVE-2024-28115漏洞原理和成因
- 1. 使用Keil自己编译部署FreeRTOS-MPU内核版本 6.1.0的固件
  - 固件除了内核自身创建的任务外，需在内核启动前创建至少以下两个目标任务
    - 一个特权任务中至少包含一个特权级的打印函数输出Attack Successfully！输出通UART QEMU的重定向到shell上。不接受任何外部输入。
    - 另外一个非特权包含一个缓冲区溢出漏洞，可溢出大小不超过任务创建时的堆栈大小，该缓冲区可接受UART的输入内容。首先需要输入和回显自己的学号。
- 2. 自己**构建攻击POC使得**在QEMU模拟器上运行的固件，通过控制流劫持，从非特权输入构建ROP攻击打印特权函数。
- 3. 替换为6.2.0 FreeRTOS-MPU内核版本任务代码和POC完全不变使得攻击失效。

- 实验提交要求
  - 1. 打包Keill工程文件夹 两个版本 以及 对应生成的固件
  - 2. 实验报告要求
    - 实验环境构建方法
    - 存在溢出的任务的栈布局
    - 漏洞存在位置和成因
    - POC构建原理
    - POC触发利用步骤
    - QEMU运行带自己学号的运行Attack Successfully!的截图
      - 模拟执行指令：./qemu-system-arm -M mps2-an386 -cpu cortex-m4 -m 16M -nographic -d in_asm,nochain -kernel 固件名称.axf -D log.txt
    - 替换内核版本后QEMU运行带自己学号的运行攻击未成功的截图
    - 说明替换后新版本对此漏洞进行了什么修复导致攻击无法成功
    - 实验心得