物联网安全复习大纲
Internet of Things Security

冀晓宇
浙江大学
2025年夏学期

期末考试说明

- 考试信息：2025-06-18(08:00-10:00)，教四-204
- 半开卷：1张A4纸双面，可以抄写或者打印，需要手写签名，考完试后上交
- 题目类型：选择、填空、计算、协议和程序分析等
- 题目覆盖上课重点讲到和作业里面的知识

各章节复习重点

物联网概述

- 掌握物联网的三个发展阶段是什么及每个阶段的特点
- 掌握本课程的物联网定义和内涵
- 掌握本课程定义的物联网三大核心特点
- 掌握物联网“云-管-边-端”架构
- 了解物联网早期形态：RFID和WSN中的关键技术
- 了解物联网的应用场景

物联网安全概述

- 第二章作为后续章节的提纲，需要：
- 掌握物联网安全定义
- 掌握物联网安全核心概念，威胁、攻击、脆弱性、风险等
- 宏观上掌握物联网“云-管-边-端”架构每层面临的安全威胁及其特点
- 掌握物联网安全的三大核心特点：
  - **“有感有控”**
  - **“AI驱动”**
  - **“业务耦合”**

古典密码学

- 重点掌握密码学中信息安全目标
- 掌握密码学体制分类，古典密码学和现代密码学的差异
- 掌握古典密码学哲学思想及其算法思路
  - 凯撒加密、仿射加密、维吉尼亚加密的机制
- 掌握古典密码学的安全性及攻击思路
  - 暴力破解、词频统计攻击等
- 了解古典密码学如何对现代密码学产生影响

现代密码学

- 掌握现代密码学的哲学思想：混淆和扩散
- 掌握私钥加密原理以及经典的DES、AES算法过程
- 掌握公钥加密思想和RSA算法
- 掌握私钥（非对称）加密和公钥（对称）加密的不同点及原因及其适用场景
- 了解密钥交换协议DH的流程及其安全问题
- 了解常见国密算法名称及对标算法
- 了解密码学的应用：数字签名、消息认证、密钥管理等
- 宏观掌握密码学在物联网中的挑战、特点和对应方法

终端安全——传感器和执行器

- 了解传感器的定义、组成、和安全相关的静态特性
- **掌握传感器测量安全**
  - 定义
  - 换能攻击定义和方法：海豚音、ghostalk、walnut
  - 换能攻击步骤：信号注入、信号生效
  - 了解防护方法
- 能利用传感器安全模型，对具体某一类换能攻击进行分析，如补全Lightcommand的攻击流图
- 了解执行器的安全攻击定义，了解常见的攻击方法

终端安全——软件安全

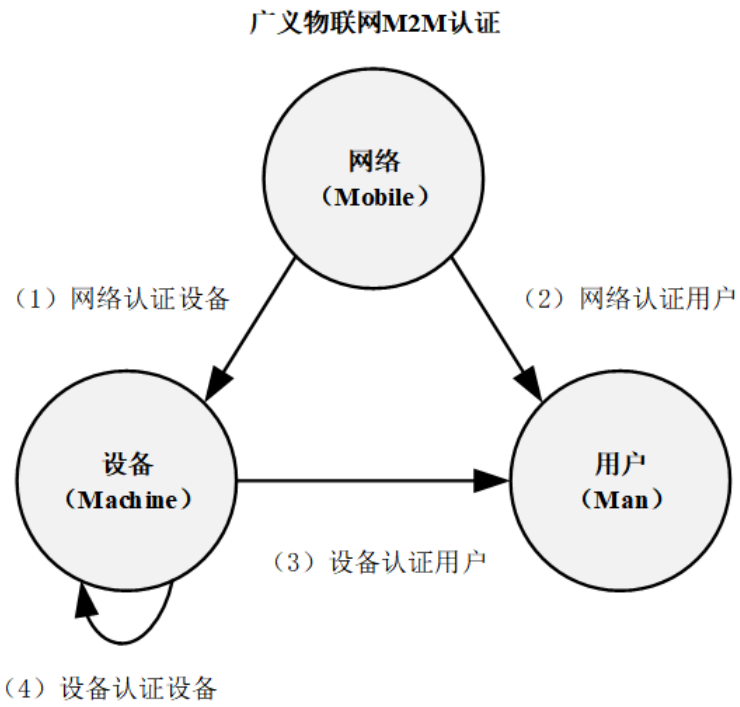
- 了解物联网软件的组成和特点
- 了解物联网固件的概念
- 物联网软件安全术语：病毒、蠕虫、木马、后门区别
- 了解物联网软件安全内涵：软件漏洞、恶意代码
- 掌握物联网安全常见的的软件漏洞，定义及类型
  - 不安全的认证和授权
  - 不安全的web接口
  - 不安全的系统和程序
- 能够综合对一个程序如buffer overflow等进行软件漏洞分析，确定属于哪种软件漏洞等
- 简单了解物联网软件安全防护方法

终端安全——芯片安全

- 了解芯片的定义、SoC
- 了解芯片的制造流程及其过程中安全隐患
- 了解物联网专用芯片代表
- 掌握物联网芯片安全威胁，每种威胁的定义、原理
  - 芯片后门
  - 硬件木马
  - 边信道攻击
  - 存储器读取攻击
- 宏观掌握meltdown芯片漏洞的利用原理和漏洞利用方法
- 了解物联网芯片安全的防护思路和方法

终端安全——认证安全

- 掌握物联网认证需求特点：轻量级、多安全等级、跨平台
- 掌握物联网认证三要素：
  - 网络（Mobile）、设备（Machine）、用户（Man）
- 掌握物联网认证技术分类体系：用户、设备
- 了解物联网常见的生物认证技术
- 掌握物联网设备指纹认证技术
  - 掌握常见的硬件指纹及其原理
- 了解物联网设备配对技术
  - 技术体系
  - 常见方法等



管道安全

- 掌握物联网管道的定义和要素
- 了解物联网管道物理链路层和应用层的代表通信协议，如5G、NB-IoT、MQTT、COAP及特点
- 掌握物联网管道在不同维度面临的安全威胁及其原因，可以对一类安全威胁进行分析
- 掌握物联网协议安全的机制、代表性安全机制的应用及其工作机理：IPSec、SSL
- 了解基于流量安全监测方法
- 了解流量安全监测学术界的典型代表工作和应用场景

语音安全

- 了解语音的基础知识和关键名词
- 掌握语音安全的内涵
- 掌握智能语音系统组成、工作流程及每个环节的脆弱性，能够对信号在不同环节中转换进行安全分析
- 宏观掌握语音识别模块的脆弱性及4类攻击内涵
- 了解ASV的攻击及防护

AI安全

- 掌握AI安全的内涵
- 了解AI的基本知识、分类模型、训练过程等
- 掌握AI安全的CIA模型、攻击者模型等
- 掌握三种针对AI攻击的定义、原理和代表性工作：
  - 数据中毒攻击
  - 对抗样本/逃逸攻击
  - 逆向工程攻击
- 掌握三种攻击的差异，并能从阶段、目标、知识要求等方面进行比较，掌握三种攻击之间的关系
- 掌握大语言模型定义、基本知识和安全威胁

边缘计算安全

- 掌握不同计算模式的差异：本地、云、边缘计算
- 掌握边缘计算模式的定义和特点
- 掌握边缘计算和云计算、雾计算的相同和差异性
- 了解边缘计算的相关技术
- 掌握边缘计算的安全威胁，尤其是能够结合边缘计算自身特点，具体分析如DDoS、侧信道攻击等具体威胁

其他

- 掌握课上学术探讨和交流的一些重要观点
  - 如传感器计算、oversensing等