物联网安全课程实验报告

**实验五**



|  |  |  |
| --- | --- | --- |
| **实验名称** | ： | RFID安全实验 |
| **姓名** | ： | 辛杰 |
| **小组** | ： | 田博仁-王梓骁-辛杰 |
| **学号** | ： | 2213034 |
| **专业** | ： | 物联网工程 |
| **提交日期** | ： | 2024年11月30日 |

## 一、实验目的

## 了解生活中RFID技术的应用及常见安全问题，了解使用Proxmark 3 RDV2对RFID卡进行安全测试的基本方法.

## 二、实验要求及要点

分组（1-3人）完成实验内容，单独撰写实验报告，回答问题，且报告内容至少包括如下要点。

**要点：**

## •实验原理及工具简介

## •实验目标与步骤（搭配实验过程照片、截图、各个卡的破解原理）

## •遇到的问题及解决办法

## •收获与感悟

## 三、实验内容

### 1、工具简介

Proxmark是一款开源的高性能RFID安全研究工具，支持低频(LF)和高频(HF)标签，兼容多种协议（如MIFARE、ISO14443、HID Prox等）。它能够对RFID标签进行读取、写入、模拟和分析，广泛应用于门禁卡、公交卡等安全测试与研究，因其灵活性和强大的功能深受开发者与安全研究人员青睐。

### 2、实验原理

1. **RFID的基本工作原理**

RFID系统包括读写器和标签。标签通过无线电波与读写器通信，分为低频(LF，125-134kHz)和高频(HF，13.56MHz)两种，频率决定了标签的通信距离、速率和应用场景。

1. **标签的数据存储与加密**

RFID标签存储的数据可能未加密或加密，实验通过读取和分析卡片通信的数据，推测其存储格式与安全机制。

1. ****标签与读写器通信协议分析****  
   通过使用工具（如Proxmark），捕获标签与读写器的通信数据，分析通信协议，识别潜在的安全漏洞（如未加密通信、弱密钥等）。
2. **攻击技术分析**

· **复制攻击**：直接读取卡片数据后，将其写入空白卡以克隆标签。

· **重放攻击**：捕获标签通信数据并在后续对读写器进行重放，模拟标签操作。

· **破解密钥**：针对加密标签，通过暴力破解或协议漏洞获取密钥以实现卡片克隆或数据篡改。

### 3、实验目标和实验步骤

#### 目标：

•学习判别RFID是低频卡还是高频卡的方法

•分别选取实验盒或生活中的一个高频卡、一个低频卡作为示例写入报告

•分析某智能门锁钥匙卡

•推测智能门锁钥匙卡工作原理

•对门锁钥匙卡进行复制攻击

•分析某小区门禁卡

•推测门禁卡工作原理

•已知小区门禁具有简单“防火墙”，对门禁卡进行复制攻击

•思考如何依赖此卡构建其他楼栋的门禁卡？

•(优先可选 )校园一卡通安全分析

•提示1：如何解密数据？

•提示2：校园卡都具有哪些功能？

•（可选）分析生活中其他常见卡

•例如银行卡、公交卡、水卡、身份证、家庭电表卡等，自行选择探索

•（可选）阅读参考资料中首次提出RFID系列攻击的论文，了解其攻击原理

#### 实验步骤：

##### 1. 判别RFID是低频卡还是高频卡

##### **2. 分析某智能门锁钥匙卡**

##### 3. 分析某小区门禁卡

## 四、回答问题

### 1）为什么不能破解生活中的RFID卡来获利？

### 破解生活中的RFID卡来获利是**非法的**，可能触犯法律（如非法获取数据或诈骗），且违反道德规范，侵害他人权益，同时风险极高，一旦被发现不仅会面临法律制裁，还可能对个人信用和职业生涯造成严重影响。因此，研究RFID安全应以技术学习和漏洞修复为目标，而非违法牟利。

### 2）假设某高校校园卡可被任意手机复制门禁功能，可能的原因是什么？

可能的原因是高校校园卡的门禁功能仅依赖**固定ID（UID）**进行验证，而不验证动态加密数据，门禁系统便只需读取卡片的UID与授权列表比对即可通过。这种设计存在严重漏洞，因为UID是静态、公开广播的，任何NFC设备都能轻松读取并复制，攻击者可将UID写入空白卡或通过设备模拟，实现对门禁系统的欺骗。

### 3）为什么学术界安全会议论文、甚至市场上的书籍会详细讨论攻击某现实应用系统的方法？有何利弊？

学术界安全论文和市场书籍详细讨论攻击现实应用系统的方法，是为了揭示潜在漏洞，提升安全意识，推动技术改进和系统升级，有助于安全生态的发展。然而，这种公开也可能被恶意者利用，导致漏洞被滥用，对未修复的系统造成威胁。因此，负责任的漏洞披露与技术探讨需要在推动进步与降低风险之间取得平衡。

## 五、实验遇到的问题

## 六、收获感悟

通过RFID安全实验，我深刻理解了RFID技术的工作原理及其安全性漏洞，尤其是如何通过分析协议、破解加密和进行复制攻击来揭示系统的薄弱环节。这不仅让我掌握了RFID卡片的读取与分析技巧，还让我认识到在实际应用中，如何设计更安全的RFID系统，以防范潜在的攻击风险。