物联网安全课程实验报告

**实验三**



**实验名称：物联网设备加密通信设计与实现**

**姓名：黄昊 孙悦 魏莎莎**

**小组：黄昊 孙悦 魏莎莎**

**学号：2110821 2110052 2112650**

**专业：物联网工程**

**提交日期：2023/11/7**

## 实验目的

了解目前主流的基于云的物联网通信原理，学会使用基本的密码学工具，并在消费物联网应用场景下构建安全加密通信方案。

## 实验要求及要点

1. 问题：
2. 智能家居设备的使用与工业控制系统面临风险有何差异？
3. 列举几种可用来实现加密通信的常见密码算法，并进行对比分析。
4. 什么是虚拟机的NAT模式、桥接模式、Host-only模式？
5. 要点：
6. 实验目标
7. 组员分工情况（须有一位组员专门从攻击者视角做安全评估，无需参与设计）
8. 方案设计
9. 方案实现（包括网络拓扑，实现技术细节，功能效果演示，等等）
10. 系统方案安全性评估（包括系统设计的不足和未来改进思路等）
11. 每位成员的收获与感悟，体会“红蓝”对抗对构建安全系统的作用
12. 提交源代码

## 实验内容

1. 基于MQTT协议，编程模拟实现智能家居应用场景下用户控制物联网设备的原型程序。原型系统至少包含如下功能：
2. 支持至少2个用户，至少3个物联网设备（空调、灯泡 、插座不同类型）同时在线

注：物联网设备硬件功能仅用代码模拟即可，如输出“on”表示灯打开

1. 在不同的实体计算机（或虚拟机、手机）上部署MQTT服务器与MQTT客户端
2. 利用密码学知识与工具，查询相关资料，使该系统能抵御指令重放攻击。
3. 模拟核心的智能家居功能：用户操控设备、查看设备状态、设备绑定。（可选功能：设备分享、设备注册）
4. 从攻击者的视角对本组的原型系统实现开展安全评估。

提示：请考虑不同的威胁模型，即不同的应用场景与敌手能力。例如，攻击者可能合法购买一个同款设备逆向分析，甚至可能共享使用过目标设备。

1. **实验过程及代码**
2. **分工情况**

方案设计：黄昊

方案实现：黄昊 孙悦 魏莎莎

安全评估：黄昊 魏莎莎

问题回答：孙悦 魏莎莎

报告整理：孙悦

1. **方案设计**
2. 设备端（device.py）：

- 设备端首先连接到MQTT服务器，并订阅用户指定的设备主题进行设备的绑定。

- 当设备端接收到MQTT消息时，会首先检查消息的时间戳，如果消息超过5秒，则忽略该消息。

- 然后，设备端会解密消息，获取设备的开关状态，并打印出设备的状态信息。

- 设备端会持续运行，等待接收新的MQTT消息。

1. 用户端（user1.py和user2.py）：

- 用户端首先连接到MQTT服务器。

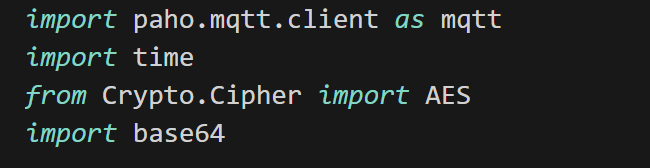
- 用户端会获取用户输入的设备状态信息，并将这些信息加密。

- 然后，用户端会将加密后的设备状态信息和当前的时间戳一起发布到对应的设备主题。

- 用户端会持续运行，等待用户输入新的设备状态信息。

1. **方案实现**
2. 设备端：

导入所需的库，包括paho.mqtt.client（用于MQTT通信）、time（用于时间戳处理）、Crypto.Cipher.AES（用于AES加密）和base64（用于编码处理）。



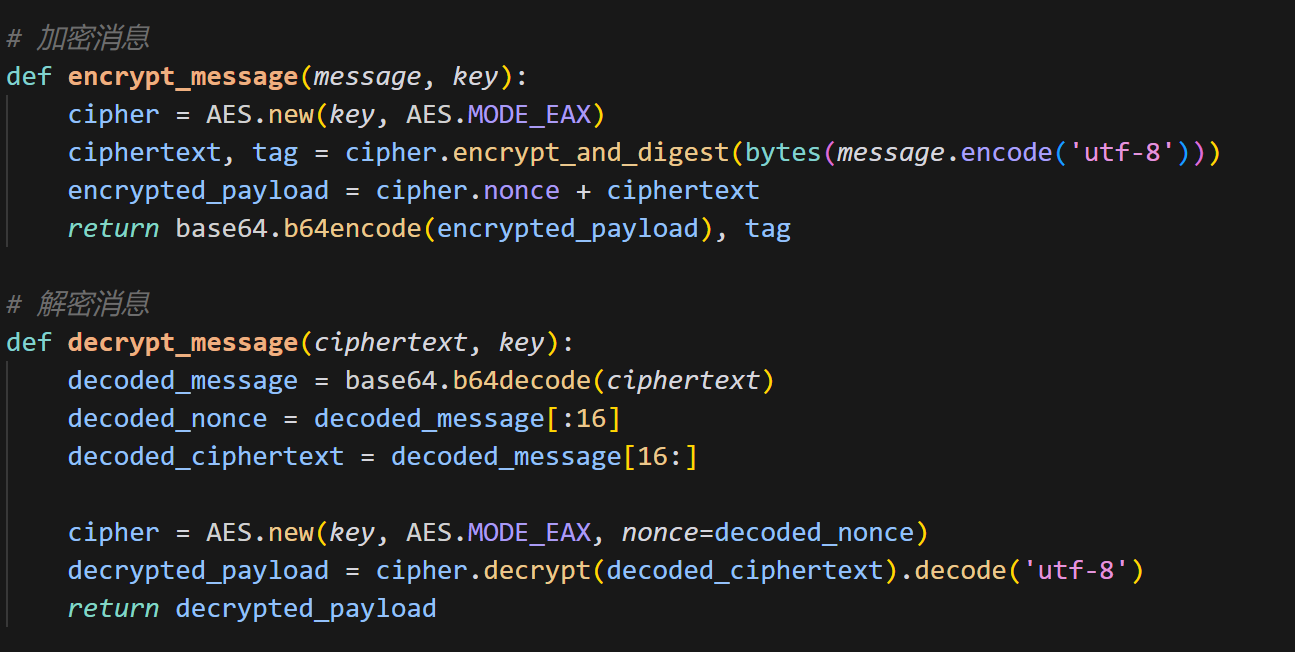
定义MQTT服务器地址和设备主题。创建一个MQTT客户端，并设置用户名和密码，然后连接到MQTT服务器。



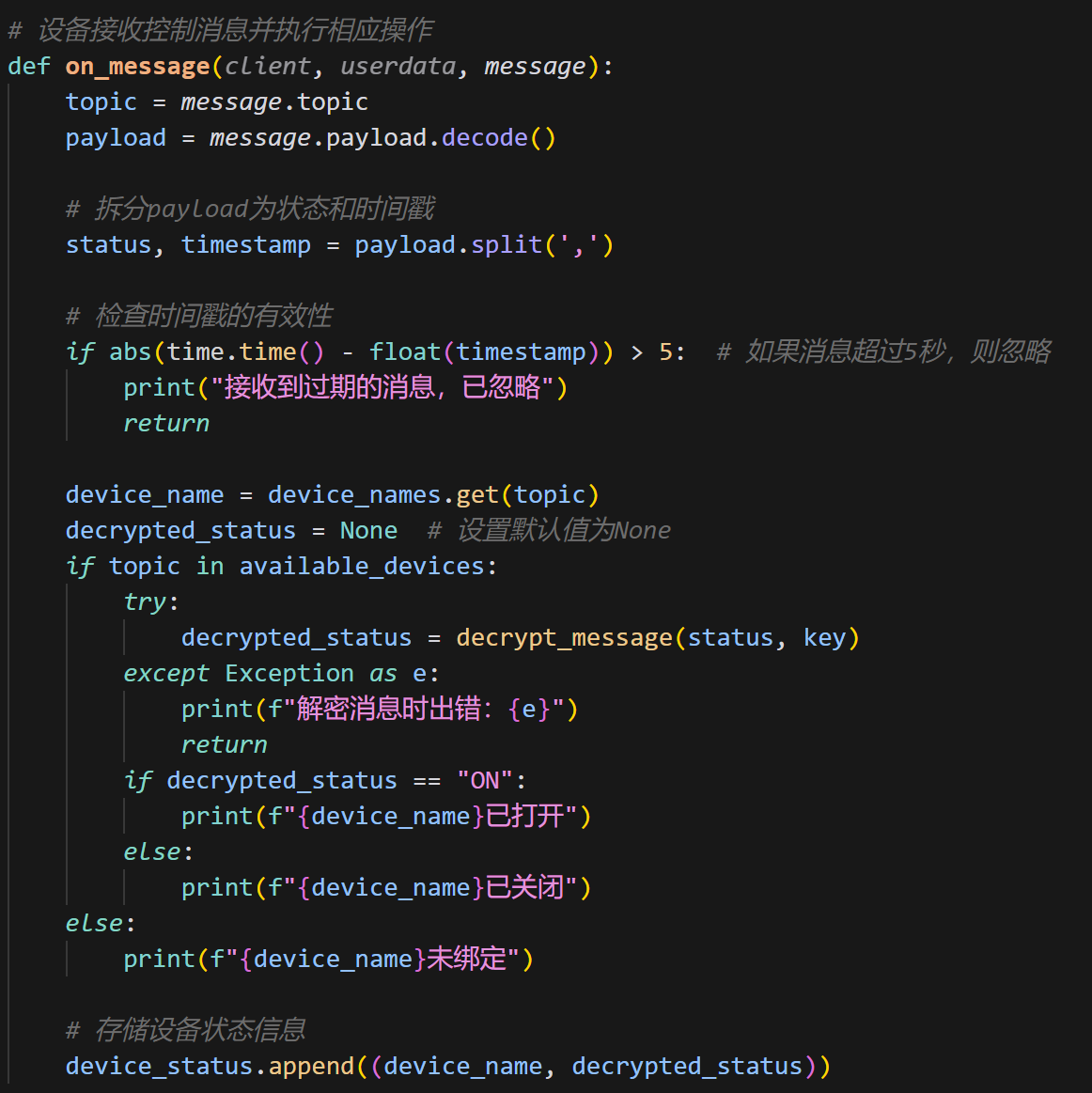
定义一个函数get\_available\_devices()，用于获取用户输入的可用设备，并将设备名称转换为对应的MQTT主题。获取可用设备列表，并定义设备名称映射和设备状态信息存储。



定义两个函数encrypt\_message()和decrypt\_message()，用于加密和解密消息。



定义一个函数on\_message()，用于处理接收到的MQTT消息。这个函数会检查消息的时间戳，解密消息，获取设备的开关状态，并存储设备状态信息。



订阅用户指定的可用设备，然后开始MQTT客户端的主循环。在一个无限循环中，检查是否有设备状态信息需要打印，如果有，则打印出来，并清空设备状态信息列表。



1. 用户端：

定义MQTT服务器地址和设备主题。创建一个MQTT客户端，并设置用户名和密码，然后连接到MQTT服务器



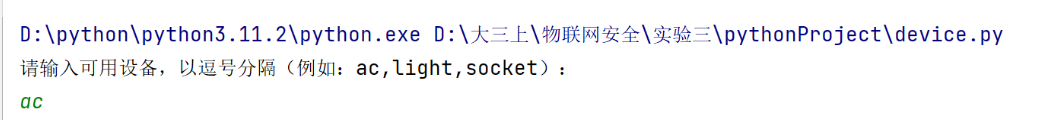
定义函数encrypt\_message()用于加密消息。获取用户输入的设备状态信息，并将这些信息加密。将加密后的设备状态信息和当前的时间戳一起发布到对应的设备主题。在循环中，获取用户输入的设备状态信息，然后进行加密和发布。



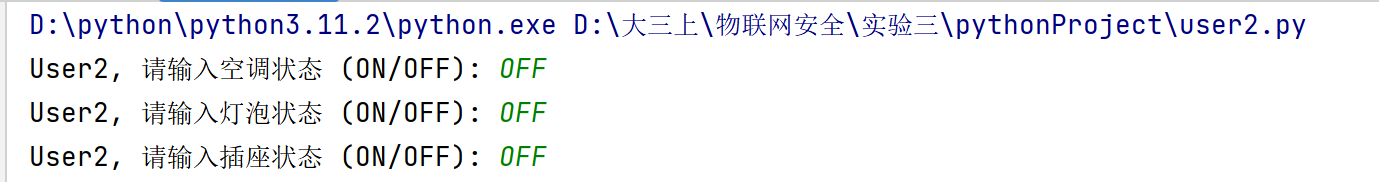
功能效果演示：

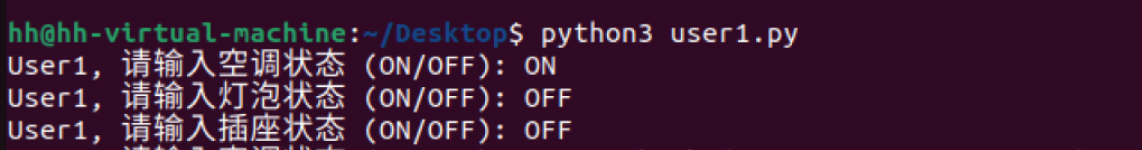
将MQTT服务器端（device.py）和用户端2（user2.py）部署在主机，用户端1（user1.py）部署在虚拟机上

用户可以输入指定的可用的设备，来进行设备的绑定



分别在主机和虚拟机模拟用户操控设备





设备端可以显示设备状态



1. **系统方案安全性评估**
2. 从攻击者的视角，以下是对本项目的安全评估：
3. 设备逆向工程：如果攻击者能够合法购买一个同款设备，他们可能会尝试进

行逆向工程，以理解设备的工作原理和通信协议。这可能会使他们能够制造假的设备，或者篡改设备的行为。

1. 消息拦截和篡改：由于项目使用MQTT协议进行通信，如果网络没有正确的

安全措施，攻击者可能会尝试拦截和篡改这些消息。虽然项目中的消息都进行了AES加密，但如果攻击者能够获取到加密的密钥，他们就可以解密和篡改这些消息。

1. 设备共享使用：如果设备被多个用户共享使用，攻击者可能会尝试利用这一

点，通过其他用户的设备发送恶意的控制消息。

1. 密码破解：项目中的MQTT客户端使用用户名和密码进行身份验证。如果这

些凭证没有正确的保护，攻击者可能会尝试破解这些密码，以获取对设备的控制权。

1. 针对以上的安全问题，以下是改进思路：
2. 增强设备安全性：可以通过硬件和软件的方式增强设备的安全性，例如使用

安全的引导程序，防止设备被篡改，或者使用硬件安全模块（HSM）来保护加密的密钥。

1. 使用更安全的通信协议：可以考虑使用更安全的通信协议，例如

MQTT over TLS，以增强消息的安全性。

1. 增强身份验证：可以使用更强的身份验证方法，例如双因素认证，以防止密

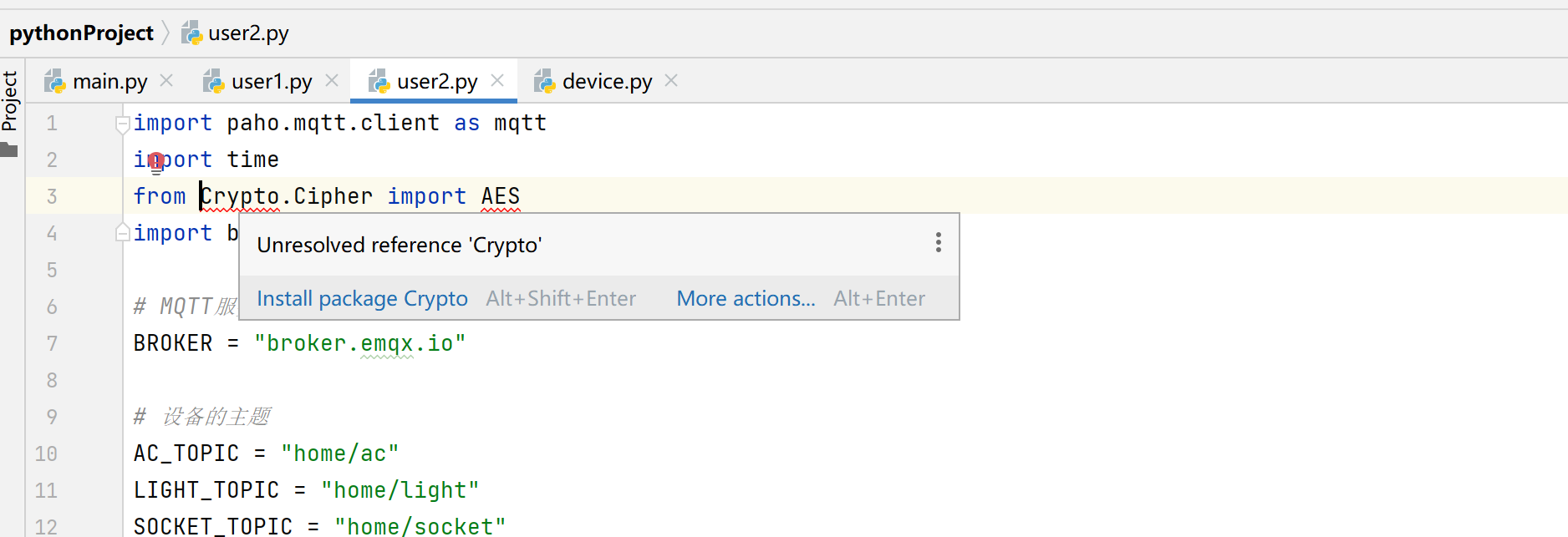
码被破解。

1. 设备访问控制：可以实施设备访问控制策略，例如每个用户只能控制他们自

己的设备，以防止设备被恶意使用。

5.遇到的问题与解决方法

1. 导入Crypto库时出现问题



解决方法：在python环境安装库的位置把里面Crypto包的名字原本首字母的小写改成大写就可以正常导入了。

1. 在cipher.encrypt\_and\_digest方法调用上，出现了函数参数类型错误：

TypeError: argument 1 must be bytes, not bytearray

解决方法：使用bytes()函数，将message.encode('utf-8')的结果转换为bytes类型。

## 回答问题

(1)智能家居设备的使用与工业控制系统面临风险有何差异？

* 目的和环境：

智能家居设备旨在提供便利和舒适，用于家庭环境，如智能灯具、智能恒温器、

智能家电等。它们主要为家庭用户设计，提供娱乐和生活便利。工业控制系统用

于监控和管理工业设备、制造过程、电力系统等，目的是确保生产的可靠性、效

率和安全。这些系统在工业环境中运行，要求高可靠性和安全性。

* 通信和网络：

工业控制系统通常使用专用网络或协议，设计用于工业环境的通信，通常不与互

联网连接。智能家居设备通常连接到普通家庭Wi-Fi网络，并且可能通过互联网

进行远程控制，这增加了网络攻击的风险。

* 安全性要求：

工业控制系统的安全性要求通常更高，因为它们可能控制重要的工业过程，故障

可能导致生产中断、损失和安全风险。因此，工业控制系统需要采取更严格的安

全措施，如网络隔离、身份验证、加密等。智能家居设备的安全性要求相对较低，

虽然也涉及到用户隐私和网络安全问题，但风险通常不会对生产过程或人员安全

造成直接影响。

(2)列举几种可用来实现加密通信的常见密码算法，并进行对比分析。

* **对称密码算法：**

常见算法：AES（高级加密标准）、DES（数据加密标准）、3DES、Blowfish等。

工作原理：使用相同的密钥进行加密和解密，速度较快。

优点：高效、速度快。

缺点：密钥分发问题，需要确保安全传输密钥。

* **非对称密码算法：**

常见算法：RSA、ECC（椭圆曲线加密）、DSA。

工作原理：使用一对公钥和私钥，公钥用于加密，私钥用于解密。

优点：无需安全传输密钥，可实现数字签名。

缺点：速度较慢。

* **散列函数：**

常见算法：SHA-256、MD5、SHA-1。

工作原理：将输入数据映射为固定长度的散列值，不可逆。

优点：快速、无法还原原始数据。

缺点：不支持加密和解密，仅用于完整性校验和密码哈希存储。

(3)什么是虚拟机的NAT模式、桥接模式、Host-only模式？

* **Bridged（桥接模式）：**

桥接模式就是将主机的网卡，与虚拟机虚拟的网卡利用虚拟网桥进行通信。

类似于把物理主机虚拟为一个交换机，所有桥接设置的虚拟机连接到这个交换机

的一个接口上，物理主机也同样插在这个交换机当中，所以所有桥接下的网卡与

网卡都是交换模式的，相互可以访问而不干扰。虚拟机ip地址需要与主机在同

一个网段，如果需要联网，则网关与DNS需要与主机网卡一致。

* **NAT（地址转换模式）：**

NAT模式下，虚拟机访问网络的所有数据都是由主机提供的，虚拟机并不真实的

存在于网络上，主机和网络中的任何机器是不能查看和访问这个虚拟机的。

NAT模式借助虚拟NAT设备和虚拟DHCP服务器，使得虚拟机可以联网。

DHCP用于动态分配虚拟机的IP地址。物理机下的虚拟网卡，在VMware下是

VMnet8网卡，在VirtualBox下不可见。另外，在连接上，虚拟机可以通过网络

访问主机，主机无法通过网络访问虚拟机，如：telnet 是连不到虚拟机中的。

* **Host-Only（仅主机模式）：**

Host-Only听名字就是只和主机建立关系。这种模式是将虚拟机与外网隔开，使

得虚拟机成为一个独立的系统，只与主机相互通讯。实现虚拟机隐藏在物理机之

后，不能上网，但可以访问物理机。

## 收获感悟

**黄昊：**

在这个项目中，我使用了MQTT协议来实现设备间的通信，这让我对这个轻量级的物联网通信协议有了更深入的理解。MQTT协议的发布/订阅模式非常适合物联网设备间的通信。它可以有效地处理大量设备的连接，并且可以灵活地处理设备的上线和下线。在这个项目中，我使用MQTT协议来实现设备的控制和状态更新，这让我体会到了这种通信模式的便利性和高效性。

同时，我也了解到，虽然MQTT协议本身是非常轻量级的，但是在实际的应用中，我们还需要考虑很多其他的因素，例如消息的安全性和设备的身份验证。在这个项目中，我使用AES加密来保护消息的安全性，使用用户名和密码来进行设备的身份验证，这让我体会到了在设计物联网系统时，我们需要综合考虑各种因素，以实现一个既功能强大，又安全可靠的系统。

此外，我还深深地体会到了“红蓝”对抗在构建安全系统中的重要作用。“红队”和“蓝队”是网络安全中的两个重要概念，它们分别代表攻击者和防御者。在这个项目中，不仅需要扮演“蓝队”的角色，设计和实现一个安全的物联网系统，还需要从“红队”的角色出发，对系统进行安全评估，找出可能的漏洞和攻击向量。这种“红蓝”对抗的过程让我更深入地理解了安全系统的设计原则和方法。我学习到，一个好的安全系统不仅需要有强大的防御能力，还需要能够预测和应对各种可能的攻击。这需要我们从攻击者的角度去思考问题，找出系统的弱点，然后采取有效的措施来修复这些弱点。

总的来说，这个实验让我更加明白，构建一个安全的系统不是一件简单的事情，它需要我们不断地学习新的知识，不断地尝试和改进。

**孙悦：**

通过本次实验，我了解了MQTT协议，以及MQTT如何工作和在程序中使用MQTT协议的发布和订阅功能；另外我还学习到了两类密码体制（对称密钥密码体制和公钥密码体制），在编写智能家居应用场景下用户控制物联网设备的原型程序过程中，我们组用到了AES加密来保护消息的安全性，使用用户名和密码来进行设备的身份验证，使系统能抵御指令重放攻击。

关于"红蓝"对抗，"红蓝"对抗是一项非常有价值的网络安全实践，对构建坚固的安全系统具有重要作用。通过这种对抗性的模拟，我们得以深刻地认识到安全系统的薄弱之处和潜在威胁。红队的攻击模拟帮助我们揭示漏洞和弱点，从而提供了宝贵的机会来改进系统的安全性。此外，"红蓝"对抗还有助于评估威胁，确定哪些威胁是最紧迫和具有潜在破坏性的。"红蓝"对抗使我们能够根据实际的演练情况来调整和改进我们的安全政策，以更好地应对不断演变的威胁。综合而言，"红蓝"对抗不仅是一项有力的工具，用于发现和修复安全漏洞，还有助于我们提高威胁感知、技能水平和团队协作，以确保我们的安全系统始终能够有效地应对不断演化的威胁。这种实践是构建强大安全系统的重要一环。

**魏莎莎：**