面向Linux物联网系统通信协议的逆向分析框架

凌 振

东南大学计算机科学与工程学院

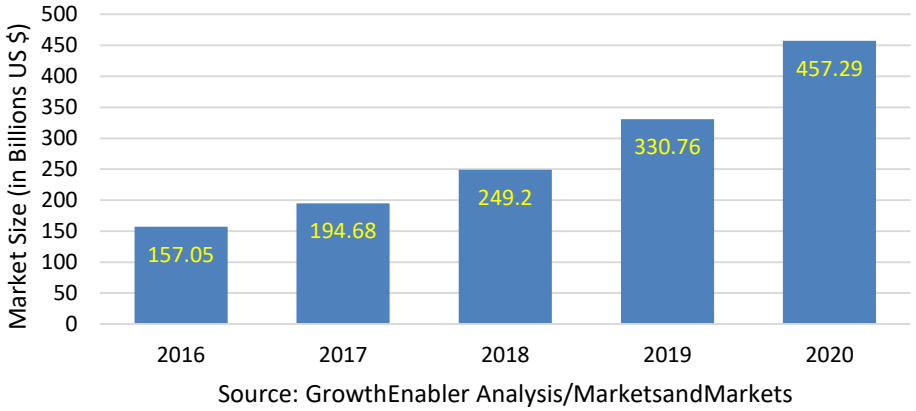
江苏省网络与信息安全重点实验室

汇报提纲

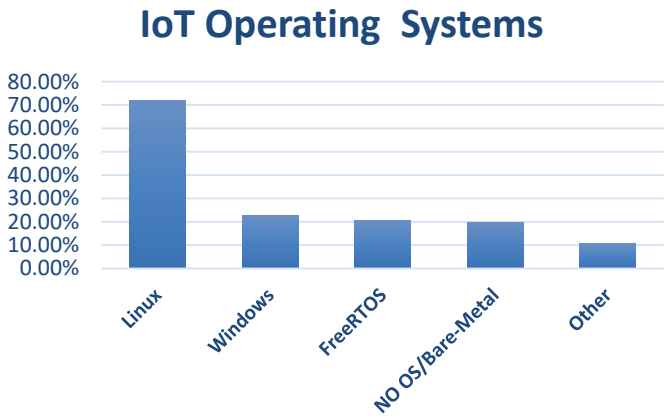
- 研究背景
- 研究现状
- 物联网协议分析框架
- 案例分析

研究背景

- 物联网设备在不同行业广泛普及，市场规模飞速增长



Source: GrowthEnabler Analysis/MarketsandMarkets



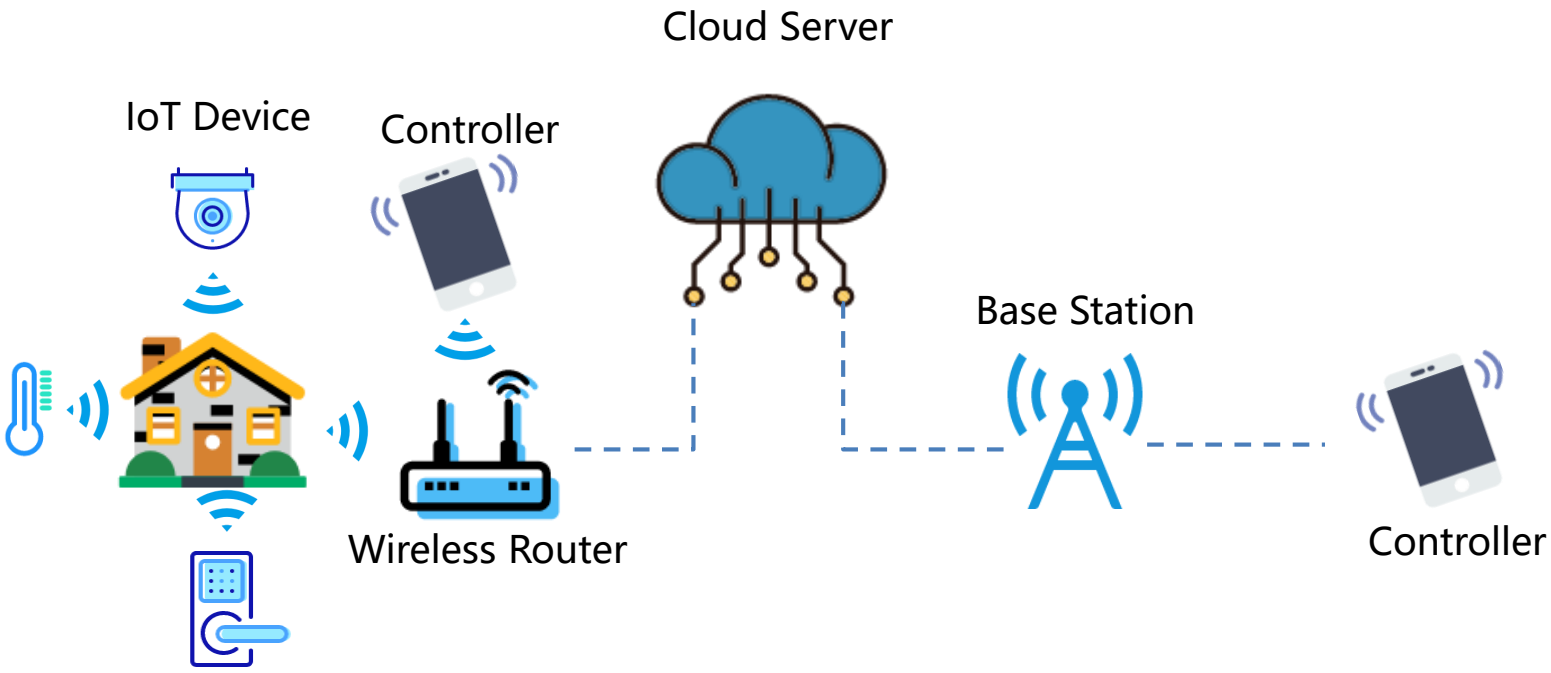
- 物联网终端存在严重的安全漏洞

2019年Amazon旗下的安防硬件产品Ring被曝出安全漏洞，黑客可以监控用户家庭，而且还会暴露用户的 WiFi 密码

2018年安全分析人员发现一种名为HNS的新型IoT僵尸网络，15天内感染了超过1.4万台的物联网设备

物联网系统架构

- 终端设备：智能摄像头、门锁等
- 控制器：安装控制APP的智能终端（如手机）
- 云端服务：提供数据转发、存储与分析功能



汇报提纲

- 研究背景
- 研究现状
- 物联网协议分析框架
- 案例分析

研究现状

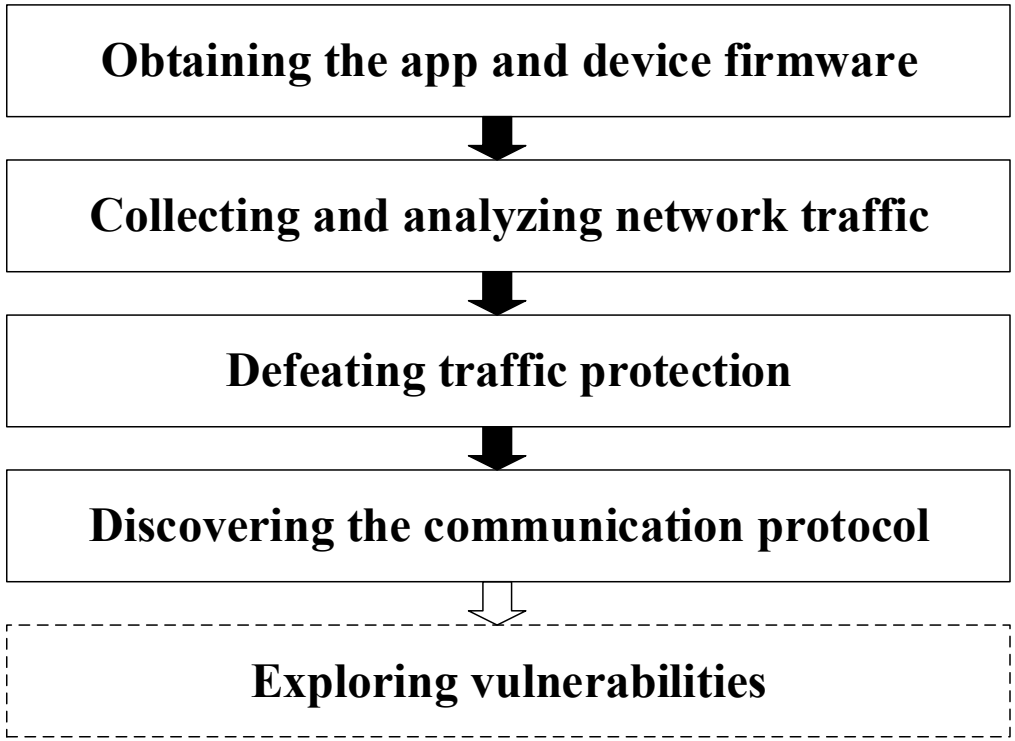
- **静态分析**
  - 通过静态分析固件，查找固件中使用不安全的配置文件（如使用自签发的证书）和程序代码中存在的漏洞（如程序后门）等安全问题
- **动态分析**
  - 解决通过虚拟机运行物联网终端固件或结合真机与虚拟机运行物联网终端固件的问题，在成功运行固件后，通过Fuzzing的方式分析固件是否存在漏洞
- **混合分析**
  - 首先利用静态分析的方法查找固件中应用程序是否存在漏洞，之后通过动态分析的方法验证静态分析结果的正确性
- **现有研究的不足**
  - 主要关注于物联网终端固件中程序代码和配置文件的安全性
  - 没有对物联网协议进行系统的分析

汇报提纲

- 研究背景
- 研究现状
- 物联网协议分析框架
- 案例分析

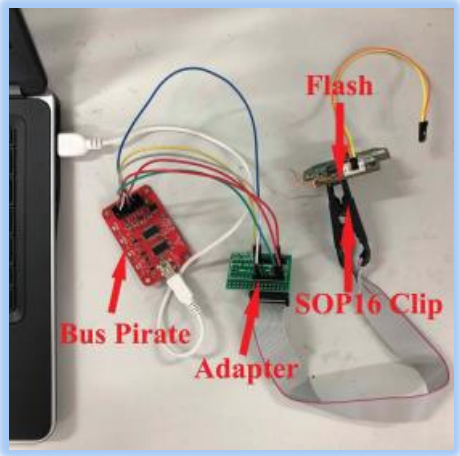
物联网协议分析框架

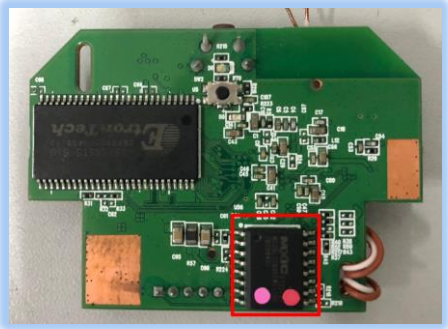
- 为了分析多样化的私有物联网协议，提出物联网协议分析框架以解析私有物联网协议
- 采用协议形式验证、手工分析等方式挖掘协议中存在的安全漏洞

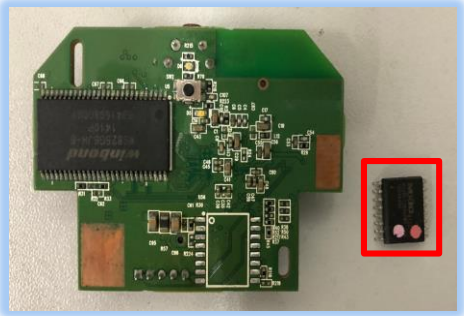


获取APP和固件

- **固件**
  - 读取Flash
    - BusPirate直接连接Flash芯片的引脚
    - 将Flash从开发板拆焊下后再用编程器读取Flash芯片
  - 分析控制器APP获取固件更新链接下载固件
  - 厂商官网下载
- **APP**
  - 应用商店下载
  - 厂商官网下载

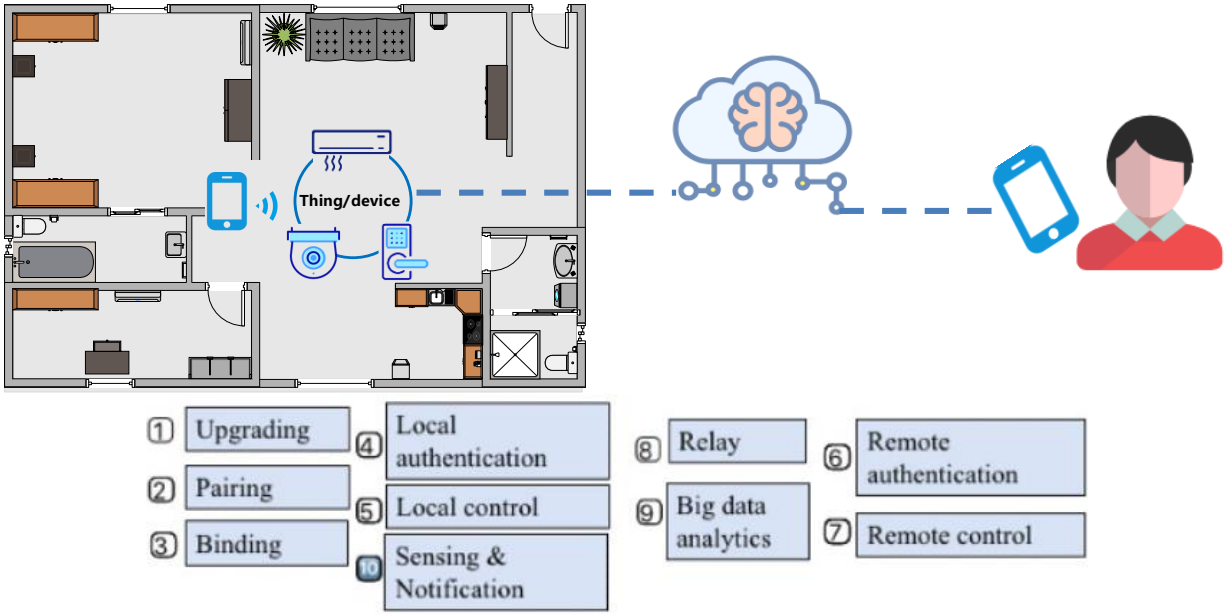






物联网协议

- **Pairing阶段**
  - 配置物联网设备连接到网络
- **Binding阶段**
  - 将物联网设备和控制器的绑定信息上传到服务器
- **Authentication阶段**
  - 服务器对物联网设备和控制器进行认证或者设备和控制器互相认证
- **Controlling阶段**
  - 控制器对物联网设备进行控制



获取与分析物联网协议流量

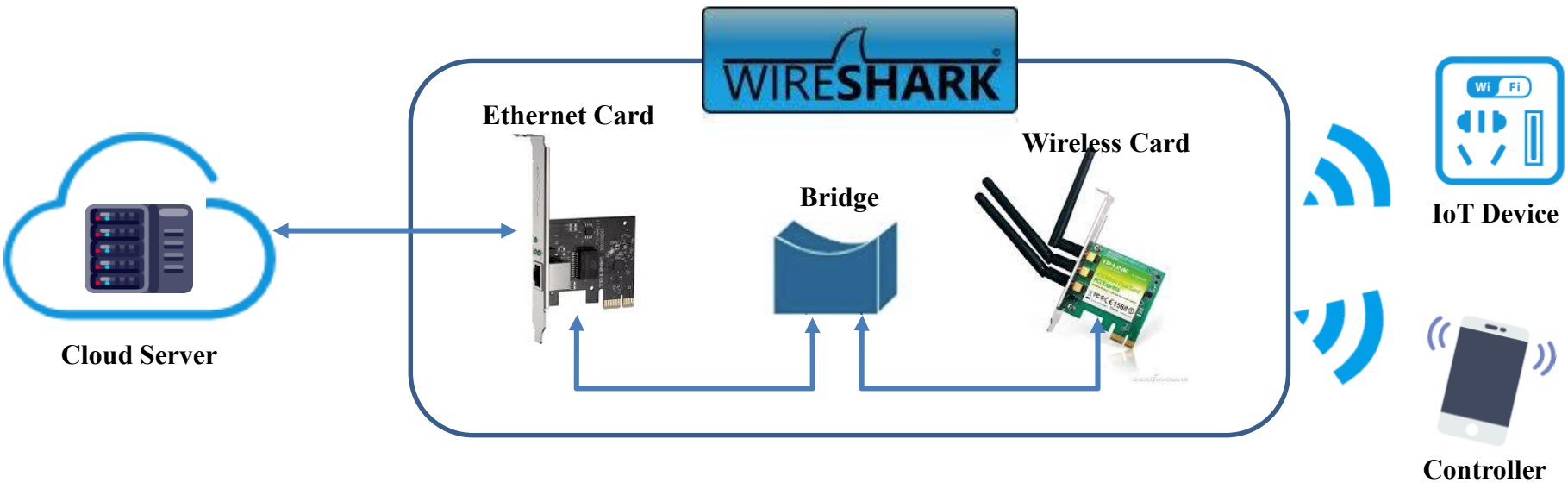
- **实验过程中发现了4种Pairing信息的传输途径**
  - Wi-Fi
    - 设备作为AP，控制器连接到设备的AP后向设备发送配置信息
  - 二维码
    - 控制器生成二维码，设备扫描二维码获取配置信息
  - 声音
    - 控制器通过声纹配置设备
  - 蓝牙
    - 控制器通过Bluetooth配置设备

获取与分析物联网协议流量

- **获取和分析Pairing阶段物联网协议的方法**
  - 逆向分析APP代码
  - 侧信道获取和分析
    - 搭建Sniffer嗅探流量（设备作为AP的Pairing方式）
    - 利用二维码解析工具解析控制器生成的二维码（利用二维码配置设备的Pairing方式）

获取与分析物联网协议流量

- **搭建网络流量获取与分析平台**
  - 解析Binding、Authentication和Controlling阶段的物联网协议

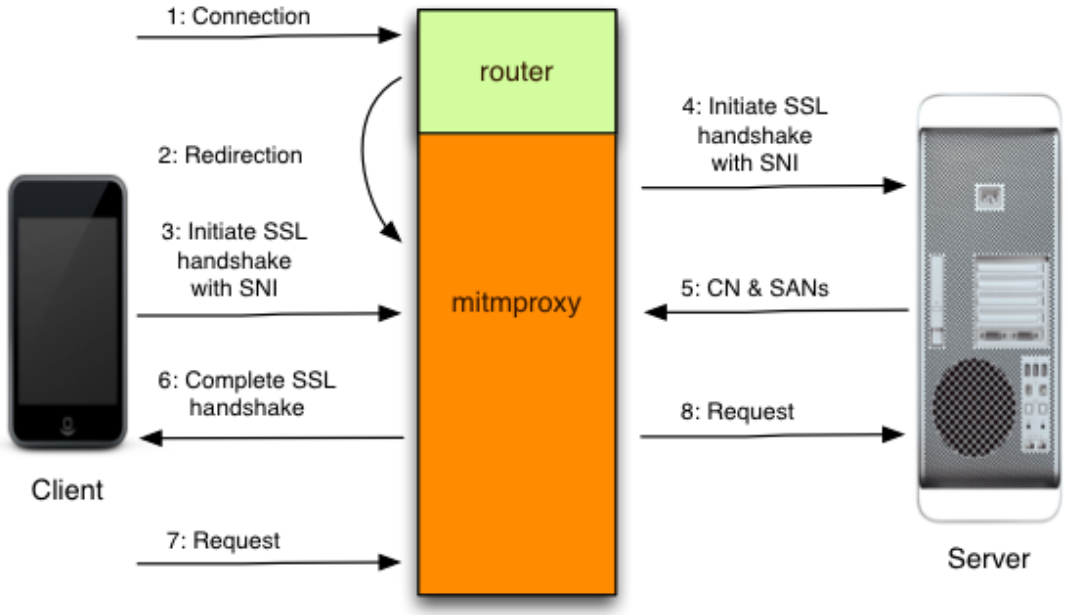


获取与分析物联网协议流量

- **通过对流量的分析，我们将物联网协议流量分类为以下情况**
  - TLS加密
  - 无加密
    - 流量应用层数据有语义（例：HTTP、XML、JSON）
    - 流量应用层数据有语义+数据混淆
    - 流量应用层数据无语义

分析加密/混淆流量

- **TLS加密流量：利用中间人攻击解密**
  - 利用MitmProxy搭建中间人攻击平台，抓取并记录解密后的流量
  - 替换/添加中间人攻击服务器证书或旁路证书校验代码



分析加密/混淆流量

- **手机端证书校验**
  - 旁路证书校验代码
    - 利用Xposed和SSLUnpinning（Exposed模块）Hook证书校验函数
  - 替换/添加中间人证书
    - 可信CA证书存放在系统证书库
      - 直接添加证书到库
    - 可信/自签发CA证书文件打包在APK中
      - 逆向分析APK，并替换证书文件后重打包
    - 可信/自签发CA证书硬编码在代码中
      - 逆向分析APK和应用程序，修改证书对应的代码，并重打包

分析加密/混淆流量

- **设备端证书校验**
  - 旁路证书校验代码
    - 利用插桩等方式Hook证书校验函数
  - 替换系统中保存的CA证书
    - 证书存储方式
      - 证书作为文件存储在系统中
      - 证书硬编码在二进制程序中
    - 证书修改方式
      - 如果文件系统可写，可以通过获取系统Shell后修改证书
      - 如果文件系统不可写或者无法获取系统Shell，可以通过修改固件中证书，重打包固件后更新设备固件实现证书的替换

分析加密/混淆流量

- **手机端混淆流量分析**
  - 定位混淆函数
    - 利用Hook（Xposed和Frida）、Debug等方法动态分析定位混淆函数
    - 静态分析定位混淆函数
  - 逆向混淆函数逻辑获取混淆算法并解析混淆的物联网协议

- **设备端混淆流量分析**
  - 利用网络传输端口号等信息定位目标应用
  - GDB Debugger和插桩等动态分析与静态分析对程序进行分析

分析物联网协议

- **解析物联网协议字段**
  - 明文字段
  - 密文字段
    - 通过熵值判断是否是密文
    - 在APP端利用Hook（Frida和Xposed）和动态调试等方法进行分析
    - 在设备端利用Debug（GDB）和插桩的方法，结合函数调用图定位和分析算法
  - 混淆字段

汇报提纲

- 研究背景
- 研究现状
- 物联网协议分析框架
- **案例分析**

案例分析

- 基于该框架分析的设备

WeMo Plug

D-Link Camera

Haier Camera

Xiongmai Camera

Edimax Camera

Edimax Plug

PurpleAir Sensor

Lenovo Camera

Yi Camera

Ezviz Camera

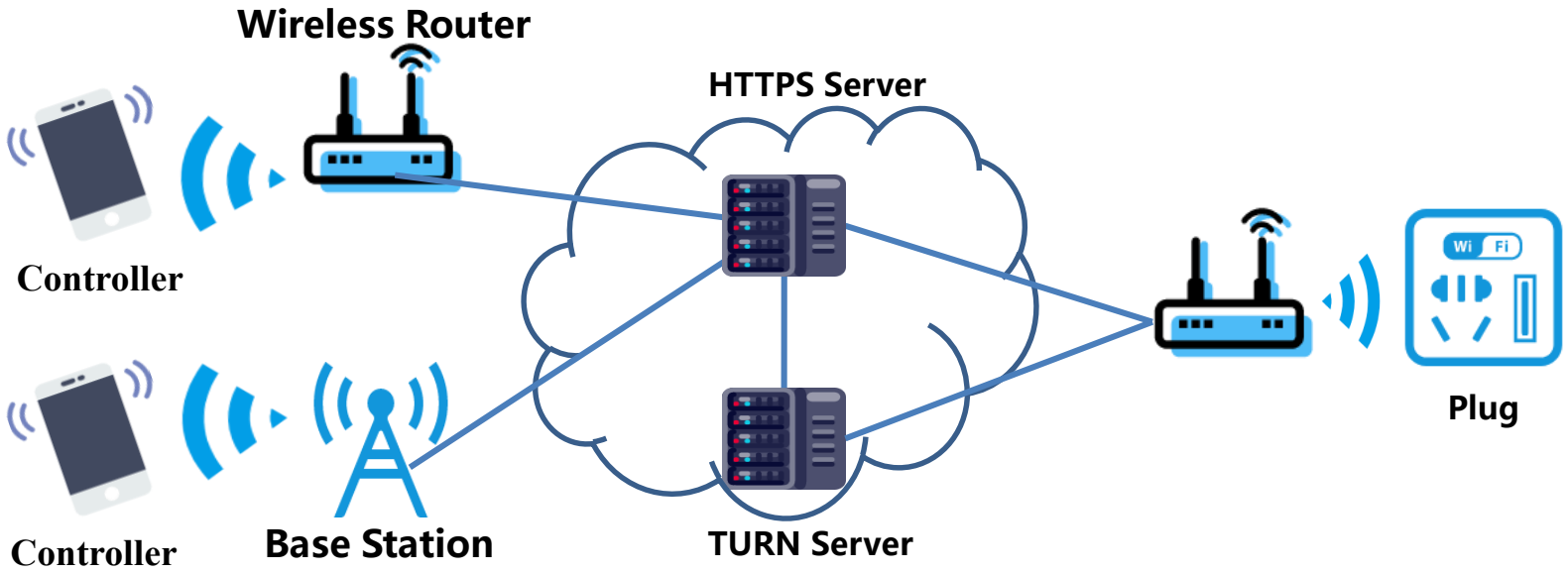
案例分析

- 设备协议分析结果

设备厂商	服务器认证控制器	设备端认证控制器	是否存在漏洞
WeMo Plug	√		√
D-Link Camera	√		√
Haier Camera	√	√	√
Xiongmai Camera	√	√	√
Edimax Camera		√	√
Edimax Plug		√	√
PurpleAir Sensor			√
Lenovo Camera	√		√
Yi Camera	√		√
Ezviz Camera	√		√

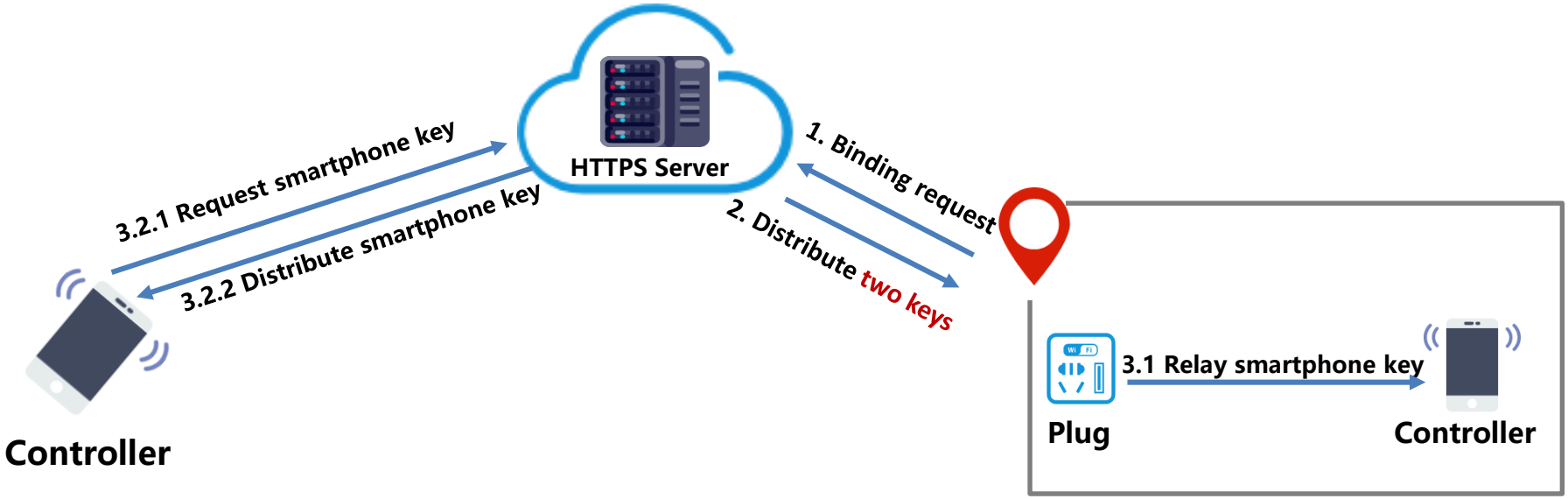
案例分析：WeMo Plug物联网协议

- **WeMo Plug系统架构图**



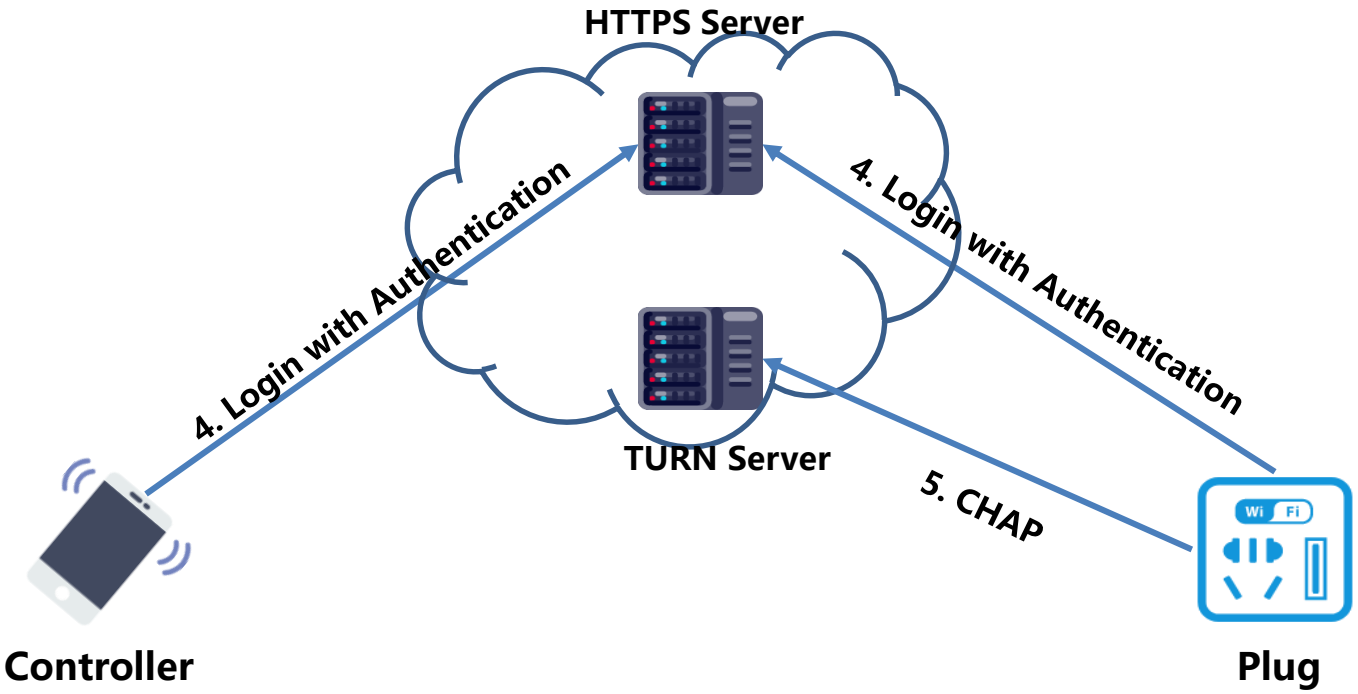
案例分析：WeMo Plug物联网协议

- **Pairing阶段**
  - WeMo Plug首先作为一个AP，用户配置控制器连接到该AP，并将控制器ID和网络配置信息发送到WeMo Plug
- **Binding阶段**
  - WeMo Plug向服务器上传控制器和设备的绑定关系，并从服务器获取控制器和设备用于计算基于HMAC-SHA1的认证字段的keys



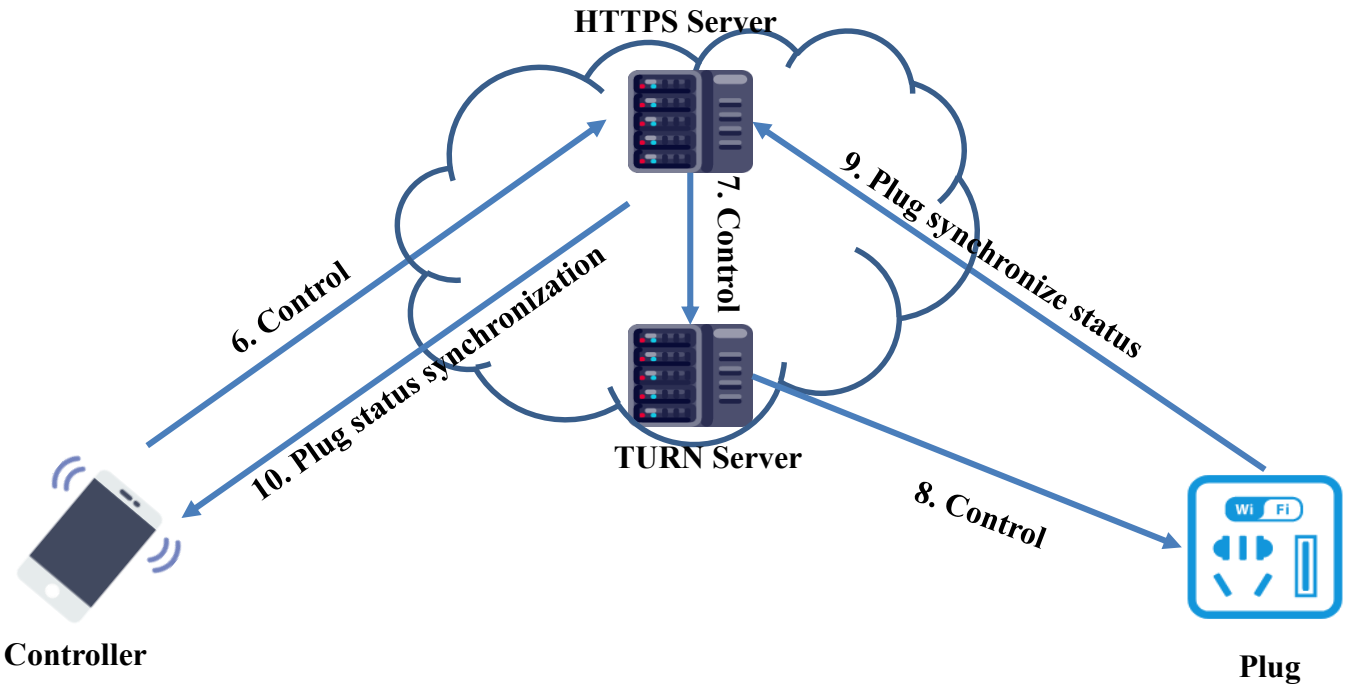
案例分析：WeMo Plug物联网协议

- **Authentication阶段**
  - 控制器和设备分别利用在Binding阶段从服务器获取的Key计算认证字段
  - 向HTTPS服务器发送包含认证字段的报文进行认证登陆
  - Plug向TURN服务器进行认证登陆，实现NAT穿越



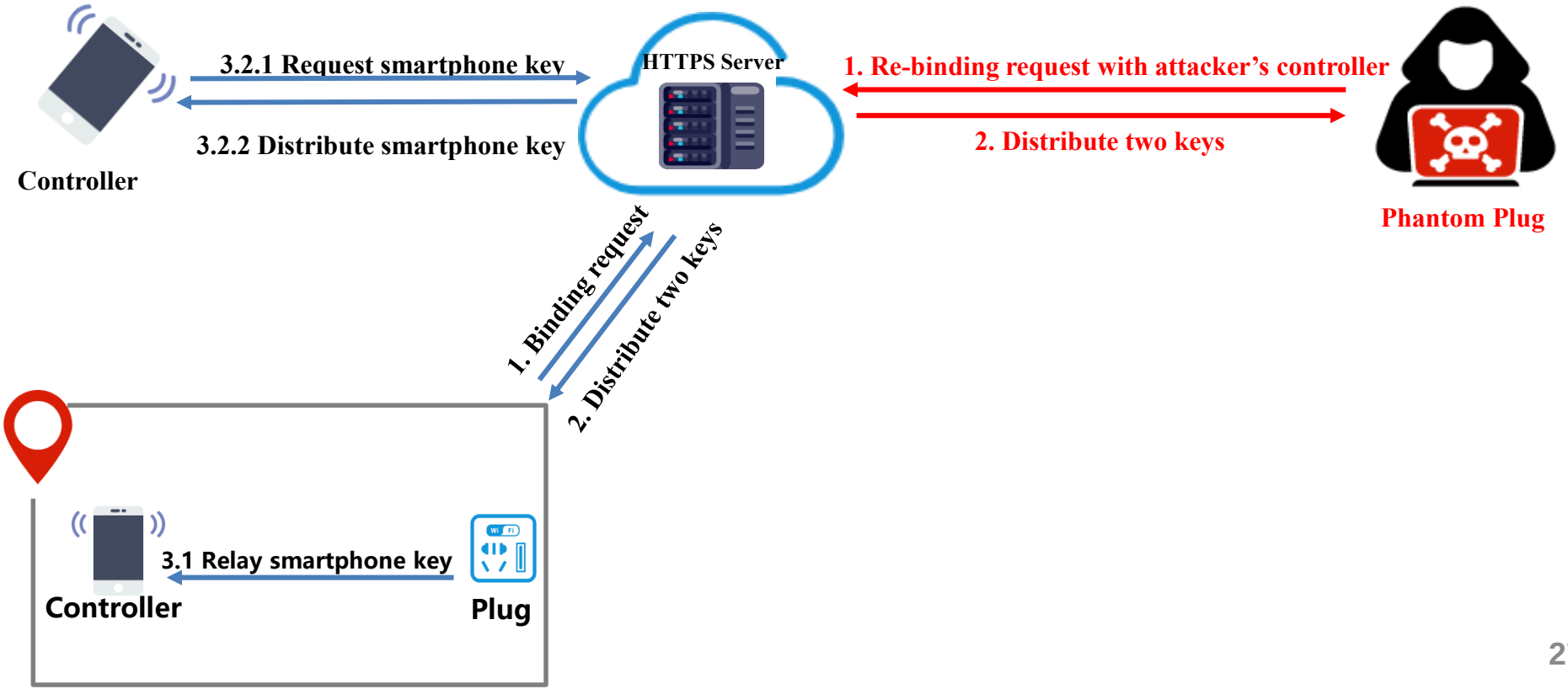
案例分析：WeMo Plug物联网协议

- **Controlling阶段**
  - 控制器通过服务器远程控制设备
  - 利用TURN协议实现NAT穿越，将控制报文转发到Plug



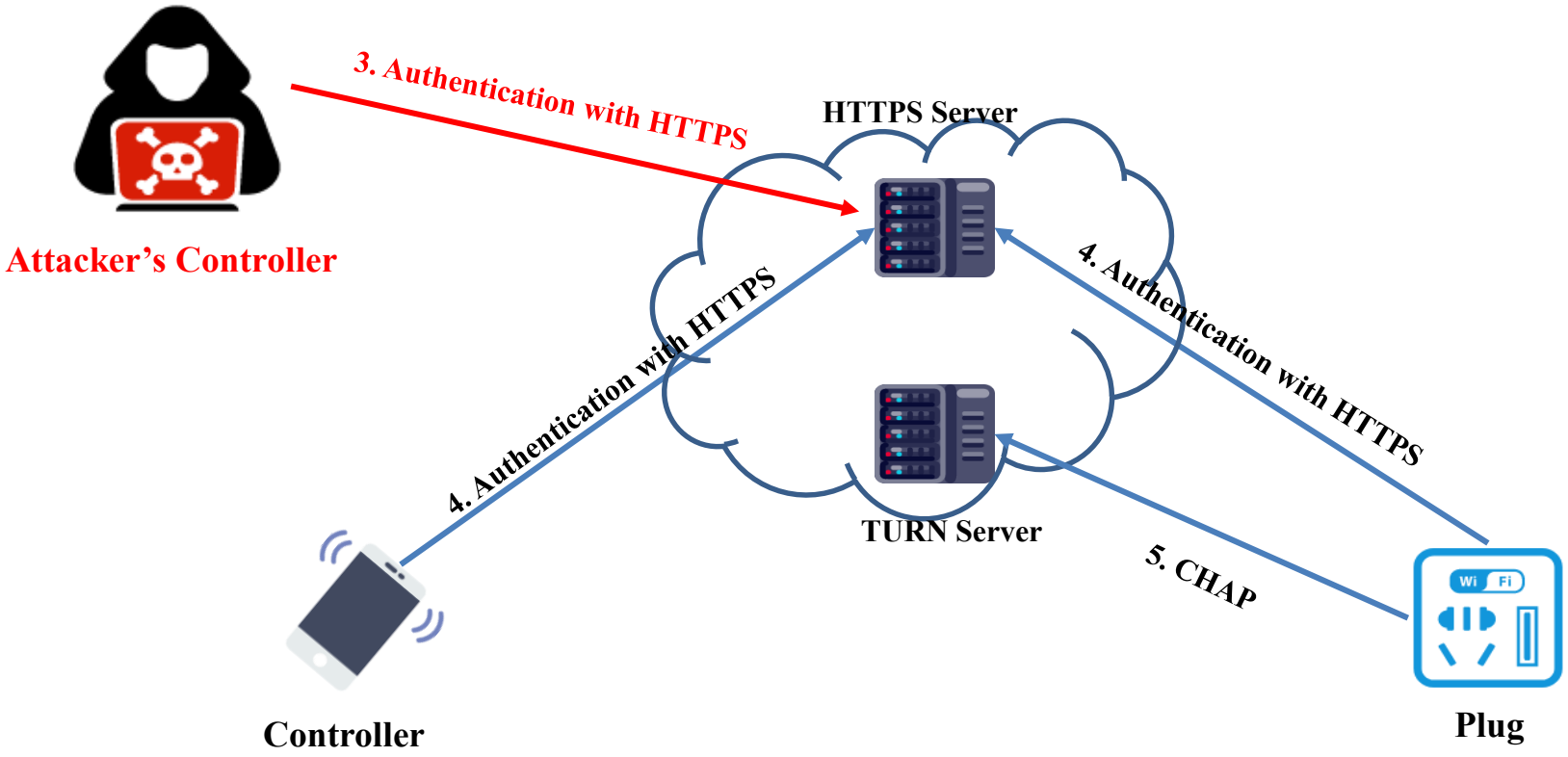
案例分析：WeMo Plug设备分享攻击漏洞

- **设备分享攻击**
  - 攻击者伪造攻击目标插座向服务器发送包含目标设备MAC地址目标设备连接WI-FI的SSID的Rebinding报文
  - 将攻击者的控制器和攻击目标设备绑定在服务器
  - 从服务器获取用于认证的key



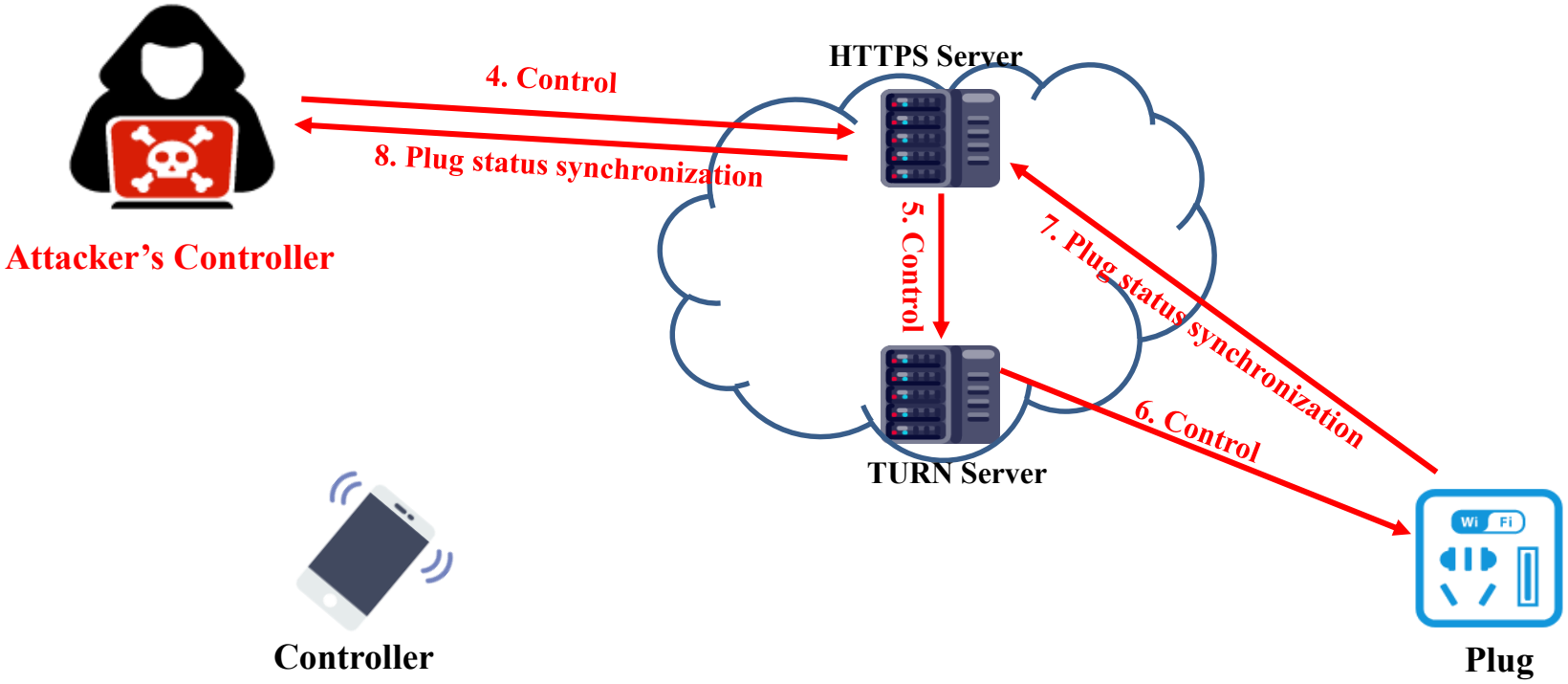
案例分析：WeMo Plug设备分享攻击漏洞

- 设备分享攻击
  - 攻击者用自己的控制器向服务器认证登陆



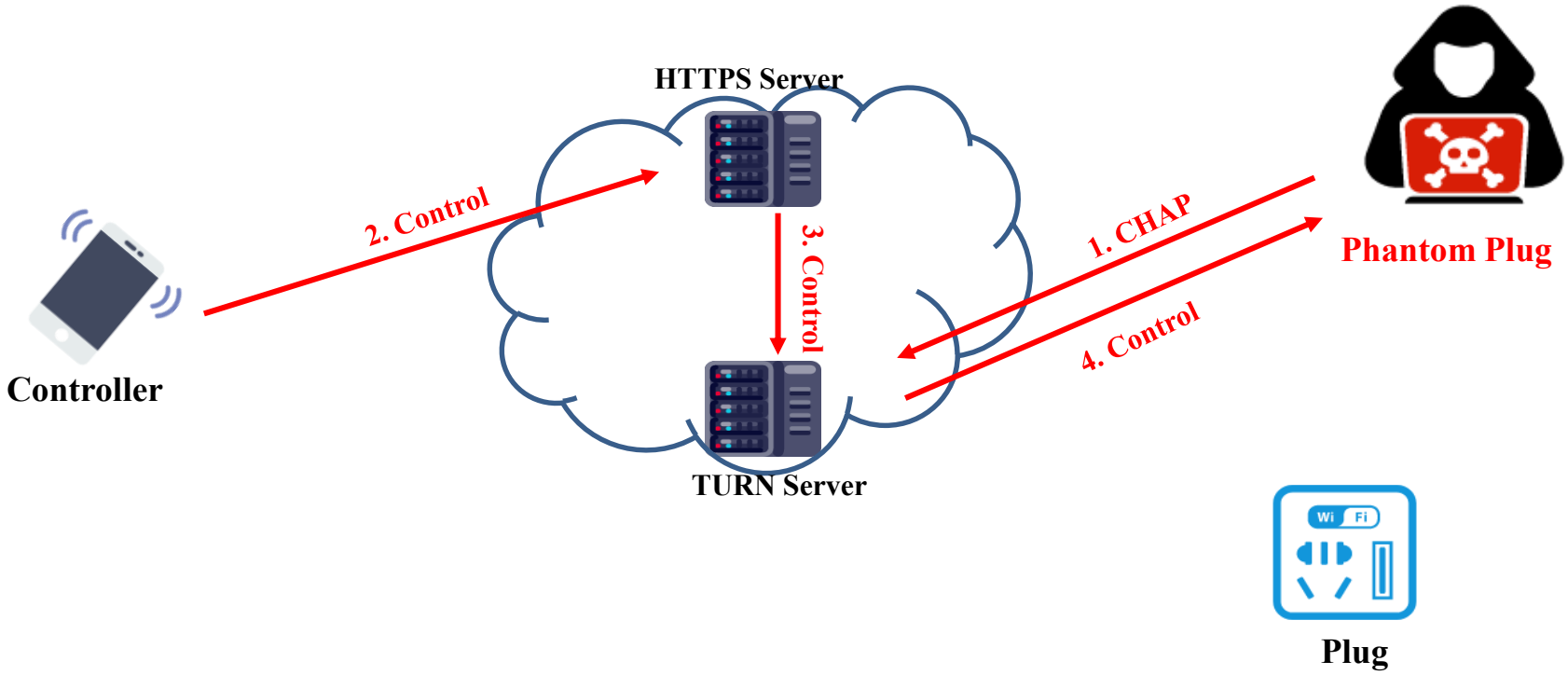
案例分析：WeMo Plug设备分享攻击漏洞

- 设备分享攻击
  - 攻击者通过云端服务器向攻击目标设备发送控制命令，实现对目标摄像头的远程控制



案例分析：WeMo Plug通信劫持攻击漏洞

- **通信劫持攻击**
  - 攻击者在设备分享攻击中可以获得目标设备用于向服务器认证的Key，利用该key攻击者可以伪造设备向TURN服务器认证登陆，从而劫持正常用户发向目标设备的报文



成果展示

- 在GeekPwn 2020成功破解雄迈摄像头和海尔摄像头

東南大學
SOUTHEAST UNIVERSITY

谢谢聆听!

凌 振

zhenling@seu.edu.cn