Deauth Flood 攻防

胡嘉鑫　　张超祥　　许诚龙　　方赞

2024 年 5 月 9 日

目录

1 实验背景

物联网（IoT）作为连接物理世界和数字世界的桥梁，已经在工业制造、运输、医疗、环境监测等领域得到广泛应用。

嵌入式系统是物联网的基石之一。它们通常是专门设计用于特定任务的计算机系统，例如传感器、执行器、智能设备等。

随着物联网规模的不断扩大，其安全问题也日益凸显。物联网的网络结构复杂，包括海量终端设备接入、各种通信协议、不同行业的安全要求等。物联网终端设备的计算和网络资源有限，这限制了复杂的安全保密协议的运行。因此，需要针对不同类型的终端设备采取不同的安全策略。物联网终端设备容易受到各种攻击，例如 DDoS 攻击、恶意程序植入、数据窃取等。因此，需要采取主动防御措施。

物联网的安全性至关重要，需要综合考虑嵌入式系统、网络安全等方面，以确保物联网的稳定和可靠运行。

2 实验目的

技术是一个不断迭代和更新的领域，随着技术的更新，系统的易用性和安全性也在不断提升。然而，现有的系统为了保持稳定性，有时缺乏定期的更新维护（尤其是嵌入式系统），这给了潜在的入侵者可乘之机。入侵者可以利用已知的漏洞对旧系统进行攻击，进行破坏、窃取信息等恶意行为，从而危及用户对系统的信任和安全。

本文重点关注无线网络安全领域，针对某一特定版本的无线网络通信协议存在的漏洞展开讨论。利用嵌入式系统来模拟攻击 (`Deauthentication Flood Attack`)，对该无线网络通信协议中的漏洞进行复现和深入研究。这样的实验和研究有助于揭示潜在的安全风险，并为加强无线网络的安全性提供有益的参考和建议。

通过对无线网络通信协议中的漏洞进行复现和研究，我们可以深入了解潜在的安全隐患以及可能面临的攻击方式。这种研究可以帮助我们识别系统中的薄弱环节，并采取相应的安全防护措施，以提高系统的抵御能力和安全性。

在当前信息技术高速发展的背景下，网络安全问题日益突出，尤其是在无线网络领域。随着物联网和移动通信的普及，无线网络的安全性愈发重要。对无线网络

通信协议中的漏洞进行研究，不仅有助于保障用户和数据的安全，也是推动整个行业技术发展的重要一步。

通过加强对无线网络安全的研究和探索，我们可以不断提升系统的安全性和稳定性，确保用户信息的保密性和完整性。唯有如此，我们才能更好地应对日益复杂的网络安全威胁，建立一个更加安全可靠的数字化世界。

3 实验环境

1. Windows 操作系统 (指挥者): 作为实验环境中的主控制中心，负责与嵌入式系统进行交互，向其下达指令并监控实验的进行。

2. ESP8266 WiFi 模块 (攻击实施者): 担当实验中的攻击者，根据指挥者的指令执行相应的操作。其主要任务是模拟 Deauth 攻击，通过向无线网络中的设备发送 Deauthentication 帧来切断其网络连接，进而影响无线网络对用户的可用性。

在这个实验环境中，Windows 操作系统扮演着指挥者的角色，通过与 ESP8266 Wi-Fi 模块进行通信来控制实验的执行。ESP8266 Wi-Fi 模块则作为攻击实施者，在接收到指挥者的指令后，执行 Deauth 攻击的操作，验证网络的弱点并评估其可用性受到的影响。这样的实验设置有助于探究无线网络安全性与稳定性之间的关系，为网络防御提供重要参考。

3.1 ESP8266 Wi-Fi 模块

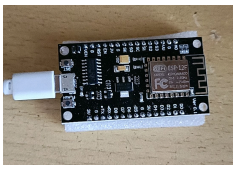

图 1: ESP8266 Wi-Fi 模块

ESP8266 Wi-Fi 模块是一种低成本、高性能的 Wi-Fi 模块，由乐鑫（Espressif Systems）公司推出。它基于 Espressif 的 ESP8266 芯片，提供了便捷的无线网络连接功能和灵活的用户程序功能。ESP8266 具有小巧的尺寸，低功耗和强大的处理能力，适合于各种物联网应用和嵌入式系统项目。

ESP8266 Wi-Fi 模块支持 802.11 b/g/n 标准，能够实现可靠的无线连接，并通过串口等接口与外部设备或主控制器进行通信。它可以作为独立的 Wi-Fi 模块，也可以作为主控制器运行用户自定义的应用程序。

由于其强大的功能和良好的性价比，ESP8266 Wi-Fi 模块被广泛应用于物联网设备、智能家居、智能设备、传感器网络等领域。开发人员可以利用其丰富的软件开发工具和社区支持，快速开发出各种创新的无线网络应用。

4 实验工具

1. `esp8266_deauther`: 来自 https://github.com/SpacehuhnTech/esp8266_deauther.
2. Arduino IDE: 介绍见下文. 我们主要使用它的编译功能, 生成可执行的二进制文件.
3. 安信可串口调试助手: Windows 和 ESP8266 WiFi 模块交互的界面.
4. `Flash Download Tool`: 用于将编译生成的二进制文件下载到 ESP8266 WiFi 模块.

4.1 esp8266_deauther

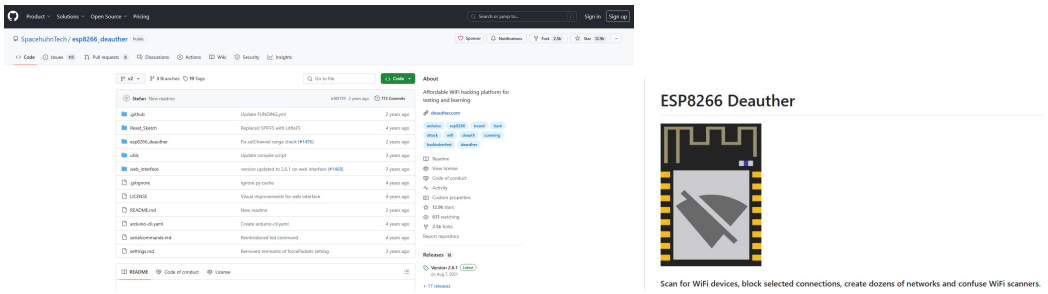

图 2: Open Source Project: esp8266_deauther

esp8266_deauther 是一个基于 ESP8266 WiFi 模块开发的开源项目，旨在实现对无线网络中设备进行 Deauthentication(Deauth)攻击的工具。通过 esp8266_deauther，用户可以利用 ESP8266 WiFi 模块向目标设备发送伪造的 Deauthentication 帧，从而迫使目标设备与 Wi-Fi 网络断开连接，造成网络服务中断或干扰。

一般来说，Deauth 攻击是一种无线网络安全测试中常见的方法，用于验证网络的弱点并评估其韧性。esp8266_deauther 提供了一个简单但功能强大的方式，让用户能够轻松地进行 Deauth 攻击，以便测试网络设备的响应能力、网络流量控制和安全性。

下面是 esp8266_deauther 的一些特点：

- 易用性：esp8266_deauther 提供了直观的用户界面，用户可以通过简单的操作选择目标设备并执行 Deauth 攻击。
- 多功能性：除了进行 Deauth 攻击之外，esp8266_deauther 还可能包含其他功能，如监视无线网络流量、嗅探数据包等。
- 社区支持：作为一个开源项目，esp8266_deauther 可能受到活跃的开发者社区支持，用户可以获取更新、修复漏洞和参与功能改进。

4.2 Arduino IDE

图 3: Arduino IDE

Arduino IDE(Integrated Development Environment) 是一个跨平台的开发工具，支持 Windows、Mac 和 Linux 操作系统。以下是 Arduino IDE 的一些主要特点和功能:

1. 代码编辑器: Arduino IDE 内置了一个代码编辑器，支持基于 C/Cpp 的编程。用户可以在编辑器中编写代码，并提供了代码高亮显示、自动补全、代码调试等功能。

2. 串口监视器: Arduino IDE 提供了串口监视器功能，用户可以通过串口监视器查看开发板与计算机之间的通信数据，便于调试和查看程序输出信息。

3. 库管理器: Arduino IDE 集成了库管理器，用户可以方便地搜索、安装和更新各种库，这些库包含了许多常用的函数和代码示例，可以加快开发过程。

4. 编译功能: 编译功能会将用户编写的代码进行预处理、编译和链接等过程，生成一个可执行文件（hex 文件、bin 文件），该文件包含了二进制形式的机器指令.

4.3 安信可串口调试助手

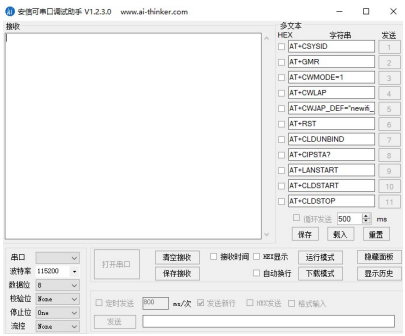

图 4: 安信可串口调试助手

安信可窗口调试助手是一款用于调试串口通信的软件工具。它能够帮助开发人员在串口通信过程中监视数据的发送和接收，进行调试和分析，从而提高开发效率和确保通信质量。

安信可窗口调试助手具有以下特点和功能：

- **串口通信监控**：可以实时显示串口通信数据的发送和接收情况，包括数据内容、发送时间、接收时间等信息，方便用户了解通信过程。
- **数据格式化显示**：支持十六进制、ASCII 等不同格式的数据显示，用户可以根据需要选择合适的显示方式，方便查看和分析数据。
- **数据记录与保存**：支持数据的记录和保存功能，用户可以保存通信过程中的数据以便后续分析和查看。
- **快捷设置**：提供简单易用的设置界面，用户可以快速配置串口参数，如波特率、数据位、校验位等。

安信可窗口调试助手在嵌入式系统开发、传感器调试、通信设备测试等领域具有广泛的应用。通过使用该工具，开发人员可以更轻松地进行串口通信调试和故障排查，提高开发效率，确保通信可靠性。

4.4 Flash Download Tool

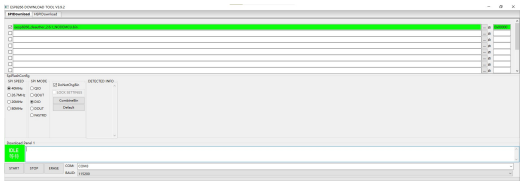

图 5: Flash Download Tool

使用时需要注意选择正确的波特率和下载地址.

5 实验原理

5.1 无线网络通信原理

何为无线网络

这里主要讲的是狭义上的无线网络, 即基于 802.11b/g/n 等标准的 无线局域网 (Wireless Local Area Network, WLAN), 由于其具有可移动性、简单性、灵活性和高扩展能力, 作为对传统有线网络的延伸, 在许多特殊环境中得到了广泛应用.

IEEE 802.11 第一版发布于 1997 年, 其中定义了介质访问接入控制层 (MAC 层) 和物理层. 物理层定义了工作在 2.4 GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式, 总数据传输速率设计为 2 Mbit/s. 两个设备间的通信可以自由直接 (ad-hoc) 的方式进行, 也可以在基站 (Base Station, BS) 或者访问点 (Access Point, AP) 的协调下进行.

1999 年加上了两个补充版本:

1. 802.11a 定义了一个在 5 GHz ISM 频段上的数据传输速率可达 54 Mbit/s 的物理层;

2. 802.11b 定义了一个在 2.4 GHz 的 ISM 频段上, 但数据传输速率高达 11 Mbit/s 的物理层.

无线网络组成

两个实体:

- 站点 (Station): 通常指无线客户端.
- 接入点 (Access Point): 无线接入点既有普通有线接入点的能力, 又有接入到上一层网络的能力. 从广义上讲, AP 就是无线路由器.

两个服务单元:

- 基本服务单元 (Basic Service Set, BSS): 网络最基本的服务单元, 最简单的服务单元可以只由两个无线客户端组成, 就好比对等网. 客户端可以动态地连接 (Associate) 到基本服务单元中.
- 扩展服务单元 (Extended Service Set, ESS): 由分配系统和基本服务单元组合而成. 这种组合是逻辑上的. 能力, 又有接入到上一层网络的能力. 从广义上讲, AP 就是无线路由器.

无线网络运作原理

无线网络的设置至少需要一个 AP, 和一个或一个以上的无线 Client 即装有无线网卡的客户端, 简称无线客户端. AP 每 100ms 将 SSID(Service Set Identifier) 经由 Beacons(信号台) 封包广播一次, Beacons 封包的长度相当短, 所以这个广播动作对网络效能的影响不大. 确保所有的 Wi-Fi Client 都能收到这个 SSID 的 AP 连接. 使用者可以设定要连接到哪个 SSID.

主要流程: 扫描 (Scan) → 认证 (Authentication) → 关联 (Association).

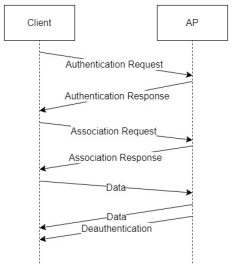

图 6: 无线网络运作原理

5.2 Deauth Flood Attack

Deauth 攻击是一种针对无线网络的常见攻击手段，攻击者利用该攻击方式可以发送虚假的 Deauthentication 帧，导致设备在接收到这些虚假帧后被迫断开与接入点的连接。这种攻击行为使得受害者无法正常访问网络，频繁断网可能造成用户体验下降、数据传输中断或网络服务不稳定等问题。

通过对 Deauth 攻击的实施，攻击者可以实现多种恶意行为，包括但不限于对特定用户进行拒绝服务攻击、窃取用户网络通信数据、诱导用户连接到恶意热点等，从而对网络安全和用户隐私构成威胁。

Deauth 攻击发生在 Wi-Fi 设备关联之后，其中引入了一个额外的实体，即攻击者（Attacker）。攻击者可以通过执行 Deauth 攻击，迫使无线接入点（AP）下的任何一个用户频繁失去网络连接，从而对其造成干扰。

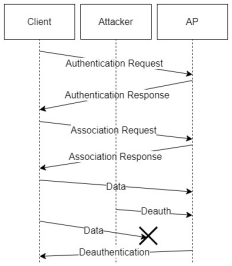

图 7: Deauth Flood Attack

在防御 Deauth 攻击方面，网络管理员可以采取一系列措施，例如使用加密通信协议、监控网络流量、配置入侵检测系统（IDS）、限制无线网络访问权限等方式来加强网络安全，减少 Deauth 攻击的影响。

6 实验步骤

6.1 攻击准备

准备硬件和软件:

- 硬件:
  - PC.
  - ESP8266 Wi-Fi 模块.
- 软件:
  - Arduino IDE.
  - 安信可串口调试助手.
  - Flash Download Tool.
  - esp8266_deauther.
  - Python-3.

下面编译生成需要在 ESP8266 上执行的固件:

```
git clone https://github.com/SpacehuhnTech/esp8266_deauther
cd esp8266_deauther/esp8266_deauther
python3 ../utils/arduino-cli-compile.py 2.5.0
```

编译完成后会得到一个 bin 文件, 需要将这个文件上传至 ESP8266, 需要用到 Flash Download Tool(需先将 ESP8266 同 PC 连接).

图 8: 代码烧录

设置完毕后点击 “Start” 开始烧录.

至此我们完成了环境的设置和代码的上传, 下面就是 “指挥” ESP8266 实施攻击.

6.2 实施攻击

6.3 结果分析

7 防范措施

8 实验总结

9 免责声明

本实验所用到的环境皆为作者个人所有, 仅作研究和学习之用. 请遵守法律法规, 其他人根据此文档进行网络攻击所造成的影响请自行负责, 与本文之作者无关!