基于WIFI网络的中间人攻击与防御技术研究

马生福　张世龙　王亦轩　王涛
西安西电安行永道信息安全技术有限公司

[摘　要]无线网络基于其便携式、灵活性、简单易操作等优势在相关领域得到了极大的推广和应用，我们要意识到无线网络在给我们带 来便利的同时，更加注重其安全隐患。本研究以探讨 Wi-Fi 网络防御技术作为出发点，分析当前常见的Wi-Fi网络攻击的过程以及原理，提出多种安全防御加固对策，旨在加强 Wi-Fi 网络的安全性，从而减少公民个人信息泄露和财产损失。最后利用Wi-Fi攻击特征提出相应的防御对策及改进措施，特别是对 Wi-Fi 使用者的安全意识提升进行详细阐述。

[关键词]WIFI网络；攻击；防护；网络安全
【DOI】10.12252/j.issn.2096-6288.2021.11.142

引言

通信技术的发展往往离不开人们对信息的需求日益增长，目前有线网络已经不能满足人们的生产生活需要，人们的目光正越来越多地投向无线网络。无线网络最典型的代表是 Wi-Fi 网络，是目前人们接触最多的无线局域网。但 Wi-Fi 网络的飞速发展带来了许多问题，其本身存在的缺陷以及漏洞，导致了许多违法犯罪情况的发生，不法分子利用 Wi-Fi 网络信道开放的特性采取特定攻击手段，窃取个人信息、商业秘密。破除 Wi-Fi 攻击带来的危机是本研究的起点。

一、Wi-Fi 网络概述

（一）Wi-Fi 网络技术介绍

Wi-Fi 网络是无线网络最典型的代表，是无线局域网的一种认证功能。当今无线局域网的通用标准是 IEEE 802.11，是由电气和电子工程师协会（IEEE）所定义的 Wi-Fi 网络通信的标准，具有 Wi-Fi 认证的产品符合 IEEE 802.11b 无线网络规范。目前最新的标准是 IEEE 802.11ax，在 2017 年由 Broadcom 率先推出 802.11ax 无线芯片。WiFi 网络采用的射频段一般为 2.4GHz 和 5GHz，其中 802.11b/g/n 定义在 2.4GHz 频段中，802.11a/n/ac 定义在 5GHz 频段中。如今越来越多的设备开始支持 IEEE 802.11 协议，Wi-Fi 网络已经不仅仅连接手机、平板、电脑等设备，在家中还可连接智能家居设备，在工厂里可以连接工控设备。

（二）Wi-Fi 网络安全技术-WPA/WPA2 加密算法

WPA 全称为 Wi-Fi Protected Access（保护无线电脑网络安全 系统），包括 WPA 和 WPA2 两种加密算法。WPA 针对政企用户和 普通用户提供了两种不同的认证方式：由于政企为保护商业机密或 者国家秘密对安全保护的要求较高，故采用远程身份验证拨入 RAD-IUS 服务器与复杂安全认证的机制，每个客户端拥有单独的身份凭 证，如图 2 所示是 WPA 政企用户认证流程；对于普通用户来说，Wi-Fi 网络通常用于上网、通讯、发邮件等对安全性要求不是很高 的功能，故采取无线接入点与终端预共享密钥（PSK）的方式保证 通信安全，所有的客户端使用相同的密钥。

二、Wi-Fi 网络安全面临的风险

（一）针对 Wi-Fi 网络的主要攻击手段

1.重放攻击 举一个简单的例子：正常情况下，主机 A 发送报文到主机 B，但是入侵者 C 从中截获了 A 发送的报文，再把此报文发送给 B，导 致 B 误认为 C 为主机 A，并把原本发送给 A 的报文发送给了 C，这 就是重放攻击。该攻击可以导致攻击者成功通过服务器的认证，进入 无线局域网。同时攻击者也可截获大量数据包，不断地重复发给接收方，造成网络堵塞，使普通用户无法正常使用 Wi-Fi 网络，导致信息 丢失。

2.拒绝服务攻击——Deauth 攻击 Deauth 攻击全称是取消验证洪水攻击（De-authentication FloodAttack），是一种典型的 Wi-Fi 网络拒绝攻击。其原理是 Wi-Fi 的管理 数据帧没有进行加密，或者若加密被攻击者破解，导致攻击者可以伪 造攻击帧，向整个 Wi-Fi 网络发送取消身份验证帧使得终端转为未认 证的状态。如果攻击者持续向网络中广播取消验证帧，就会导致终端 始终无法与无线访问接入点进行链接。

3.钓鱼攻击 钓鱼攻击的主要目的是窃取用户凭证或者用户个人信息，通常需 要搭配其他攻击来实现钓鱼目的。如目前一个主流的钓鱼攻击工具 Wi-FiPhisher，其攻击阶段分为三步：第一步，利用 Evil Twin Attack 实现了中间人攻击（Evil Twin 攻击是攻击者使用相同 SSID 创建一个 伪造 Wi-Fi 接入点，因其与原 Wi-Fi 同名，且信号一般超过原 Wi-Fi，所以更容易使用户连接）；第二步，Wi-FiPhisher 会将所有用户的 http 请求重定向，让所有使用目标 Wi-Fi 的用户访问自己的钓鱼页面。再 如 fluxion，其原理是通过 mdk3 压力攻击强制用户下线，然后伪装一 个假的无线接入点模拟原接入点，用户尝试链接时就会打开攻击者的 钓鱼认证界面，进而钓取用户的 Wi-Fi 密码。

4.暴力破解 类似于其他的密码暴力破解，Wi-Fi 暴力破解属于一种比较传统 的 Wi-Fi 攻击方式。针对 Wi-Fi 密码，攻击者利用自己的密码字典，不断尝试登录，例如：Wi-Fi 万能钥匙；针对 Wi-Fi 流量，例如对于 WPA-PSK 认证模式，可以采用字典中的 PSK+ssid 先生成 PMK 密钥 的方式进行暴力破解。

三、WIFI中间人攻击过程

将usb无线网卡插在电脑上，点击 虚拟机 -> 可移动设备 -> 选择那个有WLAN的 -> 连接，通过ifconfig命令查看网卡信息，有wlan0表示连接成功，airmon-ng start wlan0

命令开启网卡监听模式，命令airodump-ng wlan0mon，开始扫描周边WiFi网络信息。

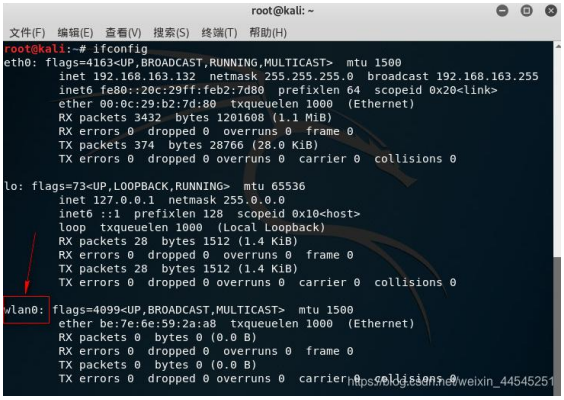

图1 看网卡信息

图2 开启网卡监听模式

接着输入airodump-ng --bssid BSSID -c 信道频率-w抓包存储的路径wlan0mon如：airodump-ng --bssid 90：8D：78：64：40：50 -c 11 -w /home wlan0mon

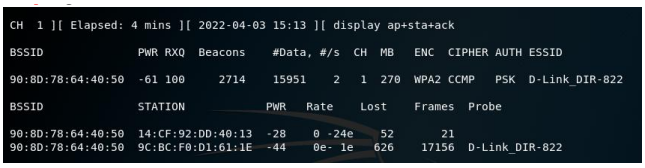

图3 抓取握手包

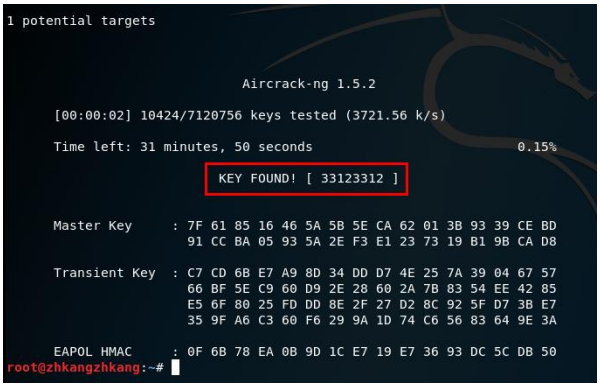

图4 WIFI密码破解成功

四、Wi-Fi 网络安全防御改进对策

（一）技术层面的改进

1.完善加密方式 纵观 Wi-Fi 网络发展史，加密方式在一次又一次的破解中而逐步 发展，从最初的 WEP 标准，到WPA/WPA2，再到如今的 WPA3，随 着解密技术的不断发展和算力的飞速提升，曾经被认为的安全加密方 式均面临被破解的风险。当今公认最安全的主流加密方式 WPA2，其 安全性是建立在使用较强的密码、通过 WPA2 认证协议加密、关闭WPS 功能的基础上的，后两点目前硬件厂商已经将其设置为默认选 项，所以基本可以保证，但对于第一点，往往是大多数人容易忽略的 地方。针对 WPA2 的破解分为两步：抓取四次握手包、对握手包进行 破解。如果用户设置的密码较为简单，入侵者是可以在较短时间内破解出密码的，这就是前面所说的 KRACK 攻击。

2.设立统一的安全标准 目前硬件厂商推出的无线接入点安全性参差不齐，如：WPA、WP2 和 WPA2-PSK 使用界限模糊，没有配置给合适的用户。即使具 有相同的安全标准，在用户的实际部署过程中也会因为配置界面不够 友好导致不会配置，更不用提让用户自行搭建 802.1 认证服务器了。所以，如何使用统一的安全标准以及如何编撰出言简意赅的配置界面，是目前硬件厂商亟待解决的问题。

（二）用户的安全意识

无论 Wi-Fi 网络安全技术发展到什么地步，人的安全意识才是保 证网络安全的基础。应当做到以下几点：

（1）使用 WPA2-PSK 认证加密。很多无线接入点会提供给用户多种加密方式的选择，选择 WPA2-PSK 加密，可有效提高密码破解的难度，降低密码被破解的可 能性。（2）隐藏接入点的服务识别码（SSID）。（3）通过服务识别码SSID，入侵者可以获取无线接入点的基 本信息，进而采取针对性攻击。通常无线接入点是默认开启SSID广播的，在部署时最好关闭广播，或者修改 SSID 广播内容。（4）使用强口令，定期更改登录密码。（5）目前 WPA2 协议被破解的关键就是在于使用了较弱的口 令，因此应使用 8 位以上、英文大小写、数字、字符混合的密码。同时定期修改登录密码，才能保证密码不会被暴力破解。（6）对无线接入点进行二次开发修改。（7）很多企业级无线接入点会提供开发接口，部署者可以利用 这些接口对接入点进行二次开发，如：采用特殊加密，修改认证界面，使用Portal认证等，模糊入侵者的攻击方向。（8）部署防火墙系统。防火墙系统可以有效地帮助用户抵御来自互联网上的病毒蠕虫 等，因为内网系统的防护往往较弱，使用防火墙系统也可以有效隔离 内网系统和互联网，防止互联网上的病毒、恶意软件等入侵内网。

参考文献

[1]黄涛，罗宁，张钦，沙琪松，孙飞虎.钓鱼WiFi检测研究及软件应用[J].科技视界，2021（15）：131-132.

[2]褚以琳.WiFi安全风险及应对策略研究[J].信息技术与信息化，2019（10）：211-213.

[3]徐国天，刘猛猛，盛振威.无线Wi-Fi环境内“中间人”攻击调查方法[J].警察技术，2021（06）：52-55.

[4]赵菁.基于Arp欺骗的中间人攻击及防范对策研究[J].网络安全技术与应用，2021（03）：6-8.

[5]黄宇，丁东，熊保国，王明，魏晓拴.基于无线信道密钥生成的中间人攻击[J].信息工程大学学报，2020，21（05）：513-519+544.