登录

WiFi安全技术　一：WiFi安全基础知识

ms0x0 / 2016-11-21 04:18:00 / 浏览数 4958 新手 入门资料 顶(0) 踩(0)

0x01 WiFi简介

智能手机的快速发展已将近十年左右，较之旧款的非智能手机，最大的区别应该是在于其强大的上网功能。在4G技术已经普及的今天，无奈国内的电信运营商们把移动联网

□
我们先解释一下WiFi这个名词。WiFi普遍的定义是一种允许电子设备连接到一个无线局域网（WLAN）的技术，有些WiFi设置成加密状态，也有些WiFi是开放的、不需要密

WiFi技术是众多无线通信技术中的一个分支，常见的无线通信技术还包括3G/4G这类基于通信基站的移动通讯技术、蓝牙、红外线连接、NFC近场通讯、射频技术等，严格的

在这里有必要特别说明，WiFi这个名词实际是代表了工业界成立于1999年的一个组织，称为Wi-Fi联盟，这个联盟致力于解决符合IEEE
802.11标准的网络通信产品生产以及设备兼容性的问题。久而久之人们习惯于用WiFi这个名词代表了无线局域网（WLAN）技术。随着科技的发展和人们对于网络的更高需
802.11标准衍生出来了很多的版本，为了便于大家的理解，我们列出了如下表所示的各版本基本信息：

标准说明802.11
发表于1997年，速率2Mbit/s，2.4GHz频道802.11a
发表于1999年，速率54Mbit/s，5GHz频道Q802.11b
发表于1999年，速率11Mbit/s，2.4GHz频道802.11c
符合802.11D的媒体接入控制层MAC桥接802.11d
根据多国无线电管理规定作出的调整802.11e
支持服务等级QoS802.11f
基站互连802.11g
速率54Mbit/s，2.4GHz频道802.11h
调整无线覆盖半径802.11i
补充安全与鉴权方面802.11n
多重I/O和40Mbit/s通道宽度，是a/g版本的延伸
除了表中列出的版本，IEEE
802.11还有一些改进型的技术，例如802.11g+或者802.11b+。不同的版本是针对不同的使用需求所做出的调整，对于我们目前常见使用的无线路由器或AP（无线接入点）
802.11b/g/n/ac版本的标准已经满足日常使用需求，并且主流无线网络设备均兼容这几个版本。为了让大家清楚直观的了解这些版本的主要区别，请看下图：

□
熟悉物理学中电磁知识的读者可能比较容易理解覆盖范围的问题，无线电频率越高，信息传输率就越高，但由此带来的电波衍射能力也就越低，因为频率越高波长越小，物理

□ 前面我们说到，WiFi的这种技术实际是无线替代有线的作用，所以WiFi的网络结构与传统有线局域网的区别并不大，下图展示了WiFi网络的常见结构：
□ 家庭网络的结构通常没有上图所示那么复杂，但基本架构不变。上图的AP（Access
Point）即相当于无线路由器的作用，有线网络通过无线路由器等设备，自行建立一个无线局域网环境，使得具备无线接入功能的设备以无线方式接入路由器内网，通过路由
Set
Identifier）发射出去，确保覆盖范围内所有的无线客户端能够收到这个SSID广播封包，并依据无线客户端的需求决定是否要和此AP进行网络连接。通俗来说，就是无线路由

0x02 WiFi网络的硬件组成

无线网络主要由基本服务单元（BSS）、站点（station）、接入点（AP）、扩展服务单元（ESS）组成。这里特别说明，在破解WiFi密码的过程中，BSS可以简单理解为无线

组建一套基本的WiFi网络环境，最常见的就是无线路由器和具备无线网卡的上网终端。无线路由器和无线网卡将传统的有线局域网络转变为方便人们使用的WiFi网络。这里我

□
无线路由器和普通的有限路由器并没有本质上的不同，额外多出的天线，将网络信号以无线电方式向外发送出去。无线路由器可以视为是将单纯的无线接入点和路由器二合一

无线网卡可以是单独的一个设备，也可以集成在例如手机、平板电脑、笔记本电脑等具备无线联网功能的终端中。市场上常见的无线网卡有USB接口和PCI接口两种，下图是

无线网卡的功能比较简单，连接终端后以无线电的形式与无线路由器相配合，接收与发送网络信号，形成网络通信媒介。无线路由器和无线网卡的通信都基于802.11标准，都

网络设备的生产商不会只局限于生产某一种设备，同品牌的无线路由器和无线网卡产品在市面上层出不穷，扩展功能也是创新不断。目前国内流行的无线网络产品品牌有TP-

在具有针对性的WiFi网络入侵案例中，无线设备的发射功率是一个重要的考量标准。如何在更远的距离上获取更稳定可靠的通信线路一直是无线黑客们追求的目标。在这里

无线网络设备的天线有外置式的，比如上图中伸出的天线，也有内置式的，比如集成在手机里的天线。天线分为全向天线和定向天线两种，简单可以解释为，全向天线的信号

在这里需要提醒大家的是，所谓的大功率蹭网卡，虽然装备有定向天线，发射功率也比较大，但很多时候并不适用于连接较远距离的无线路由器或者AP。无线网络通信的稳

0x03 必知的一些名词和术语

SSID：Service Set
Identifier，服务集标识符。用来标识某一无线局域网的唯一标识符，无线客户端用它入网后与接入点进行通信。SSID是人为可设置的，大家在设置无线路由器的无线信号时

WAP：Wireless Application Protocol，无线应用协议，利用它可以把网络上的信息传送到移动电话或其他无线通信终端上。
AP：Access Point，无线访问点或接入点。客户端需要连接AP才能获得登录互联网的能力。具备路由功能的AP就是一个无线路由器。 WEP：Wired Equivalent Privacy，802.11定义下的一种加密方式，是常见的一种无线网络的认证机制。这种加密认证机制基本已经被淘汰，是一种WiFi早期使用的加密方式，目的是给无线网络传输ping算法。
WPA：WiFi Protected Access，常用的无线网络认证机制之一，有WPA和WPA2两个标准，并且分为个人和企业的WPA-Personal和WAP-Enterprise两种。它是为了完善WEP加密方式的安全性不
Station：站点，网络最基本的组成部分，通常指接入网络的无线客户端，例如手机、笔记本电脑、平板电脑等。
BSSID：基本服务单元ID，在无线安全审计软件中通常显示为接入点的MAC地址。SSID和BSSID不一定一一对应，
一个BSSID在不同的信道上面可能会对应到多个SSID，但在一个信道上它们是一一对应的。
信道：Channel，是对频段的进一步划分，比如2.4G的频段范围再划分为几个小的频段，每个频段称为一个信道，处于不同传输信道上面的数据，如果覆盖范围没有重叠，
信道宽度：Channel Width，例如有20MHz、40MHz等，表示一个信道的宽度。
抓包：将网络传输发送与接受的数据包进行截获、重发、编辑、转存等操作，在我们讨论的WiFi安全中，通常指无线数据包的截取等。

0x04 简单案例、防护提醒

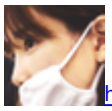
家庭无线网络被攻破：

目前几乎每个家庭都有WiFi网络，已经成为生活中不可缺少的一部分。由于家用无线路由器的信号范围能够达到几十米，那么周围的邻居、楼下停车场的路人都有可能搜索到

企业无线网络被攻破：
如果一个企业的无线网络被攻破，通常情况下，攻击者能够顺利的加入内网环境，访问公司内部网络敏感资源，或者直接渗透进入敏感部门人员使用的计算机获取重要文件等

WiFi的安全问题并不只有上述两种危害，在这里给大家先行提醒几个降低WiFi安全隐患的几点建议：
手机在不用WiFi时将WiFi功能关闭，需要时手动打开，可以避免连接设有陷阱的公共钓鱼WiFi信号，造成手机存储的一些敏感数据被盗。
避免在公共场所，例如火车站、机场、商场等地使用密码公开的公用WiFi。此时你和不怀好意的攻击者处于统一内网，很容易被进行钓鱼或者网络劫持。
自用的WiFi，SSID最好设置成中文名称，可以减低被破解的风险，因为国外的很多破解软件并不支持中文，会存在乱码问题。
自用的WiFi密码一定要设置的足够复杂，甚至像乱码一样，避免使用12345678这类弱口令，以及和家庭成员有关的密码设置，比如手机号、门牌号、姓名拼音等作为密码。
经常查看无线路由器的管理页面，查看有没有非授权用户接入自己的WiFi网络。
如果可能，在公共外出场所尽量使用手机数据流量进行上网，尤其是使用支付宝、登录某种账户等操作时，免费的WiFi总有可能会带来不安全的因素。

上一篇：一个漏洞批量验证的小工具HackU... 下一篇：【技术分享】使用反序列化漏洞干掉你...
1. 1 条回复


hades 2016-11-21 04:54:46

楼主，请完善标题和内容

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录