Wifi安全技术

WiFi是IEEE（电气和电子工程师协会）定义的一个无线网络通信的工业标准IEEE802.11。可以将个人电脑、手持设备（IpDA、手机）等终端通过无线方式互相连接的技术。

近年来，睡着无线网络技术的成熟，越来越多的人们通过无线设备连接到互联网。最早的wi-fi只用于对IEEE802.11b系列的产品进行认证的描述，全称为wireless-fidelity，但现在正在逐步扩展到802.11系列的各类标准，用户也开始使用wifi或者wifi指代所有的无线网产品标准。

当前无线网用户对于随时随地访问自己关心的网络数据要求越来越高，为此，各类场所对无线网的部署也日益流行。布置方有家庭、企业还有运营商，但是无论何种规模的无线网，都面临着各种各样的安全隐患和威胁。

WiFi上网的安全隐患中，最最重要的还是在连接了无线网络后的个人信息的丢失。黑客是如何在公共场所盗取用户信息的呢？第一，黑客可以通过内外攻击软件在设备和路由之间伪造中转站；2、使用内网广播的机制，监控上网流量，从而找到你的浏览记录3、伪造Wi-Fi广播，比如将SSID设置为一种常见的公共Wi-Fi，当你连接时，设备便有可能被植入木马或是间谍软件，等等之类的。

网络安全研究机构进行了WiFi 不安全的原因分析，结果显示:密码设置简单占第一位，高达35%;其余的原因分别是:工具暴力破解30%，路由器漏洞15%，透露密码和蹭网软件共享各占10%。目前，无线局域网发展过程中遇到的最关键问题恐怕就是安全问题了。与有限局域网相比，无线局域网所增加的安全问题主要原因，是由于其利用公共的电磁波作为载体进行传输数据信号引起的。

由于无线局域网利用无线电波传输数据的过程是在空中完成的,可以说在数据发射器所能覆盖的区域范围内，所有无线局域网用户在任何一层楼、一个房间内都是可以搜索接触到这些数据信号的。这意味着想将无线网发射出的信号只传送给某位特定的接收者是不可能实现的。又因为防火墙对利用无线电波进行传输数据的网络通信不起作用，所以任何人在信号覆盖范围内都可以拦截和插入数据。

目前wif无线网络的蹭网现象非常普遍,为了防止未经过允许的用户使用自己的wifi无线网络，无线局域网在编制程序时加入了一些安全防范措施。一般情况下wifi无线网络的安全防范措施主要针对两个方面: -是对网络程序进行加密;二是对用户访问权限的制约。访问权限的制约是确保只能由授权的用户进入自己的网络，而网络程序的加密则使得发送的信息能更准确地到达希望接收的用户，保证发送过程中不被其他用户盗窃和拦截。

对于无线网络安全性能有些什么要求呢？

在无线网络中，信息在被授权的用户之间交换，由于无线介质的广播性质，该传播过程很容易受到各种恶意威胁。无线网络的安全要求为保护无线传输与无线攻击而指定，如窃听攻击、dos攻击、数据篡改攻击、恶意节点的攻击等等。一般来说，无线通信的安全应该满足真实性，保密性，完整性和可用性的要求。

（1）真实性：指确认网络节点的真实身份,以区分授权用户和未经授权的用户。在无线网络中，一对通信节点在建立数据传输的通信链路之前应首先进行相互认证。通常情况下，网络节点配备了无线网络接口卡,并具有唯的MAC 地址，可用于身份验证的目的;再次，除了MAC身份验证外,还有其他的无线认证方法,包括网络层认证、传输层认证和应用层认证。

（2）保密性:指只限制预期用户的数据访问，同时防止信息泄露给未经授权的实体。以对称密钥加密技术为例,源节点首先加密原始数据(通常称为纯文本)，使用一个仅与目的地共享的加密算法和密钥;其次,加密的纯文本(称为密文)发送到目的地,然后使用密钥接收文本，由于窃听者不知道密钥，它是无法偷听的密文的明文的。

（3）完整性: 指在整个生命周期中源信息未被未经授权的用户进行任何修改和伪造。数据完整性可能遭受所谓的内部攻击，例如,节点妥协攻击，更具体地说，一个节点被攻击时，节点可能会因为恶意攻击包括消息注入、虚假报告、数据修改等损害数据的完整性。一个有效的解决方案,通过利用自动代码更新检测受损节点，以保证受损节点被定期检测到。

（4）可用性:指授权用户能够随时随地访问无线网络的要求。违反可用性，称为拒绝服务,将导致授权用户成为无法访问无线网络，这反过来又导致不满意的用户体验。

综上所述，无线网络的安全性能要求应该和有线网络一样，包括真实性、保密性、完整性和可用性的要求。然而，由于广播的广播传播的性质，实现这些无线网络中的安全要求比有线网络更具挑战性。例如，无线网络的可用性是非常脆弱的，因为施加的无线电信号的干扰攻击，可以很容易的破坏和阻断无线物理层通信。因此，与有线网络相比，无线系统的安全性能面临更高的要求。

对于无线局域网络主要有以下几种安全措施

1.过滤无线网卡MAC。

每个无线工作站网卡都需要用惟一的、以48位编码的物理地址表示。因此在无线网访问点AP中可以设置-组需手工维护的MAC地址列表，来自行决定是否允许访问，以达到对物理地址的访问过滤目的。

无线MAC过滤原理

选择菜单无线设置→无线MAC地址过滤，您可以查看或添加无线网络的MAC地址过滤条目。

无线mac 地址过滤功能通过mac 地址允许或拒绝[无线网络](https://baike.baidu.com/item/%E6%97%A0%E7%BA%BF%E7%BD%91%E7%BB%9C)中的计算机访问[广域网](https://baike.baidu.com/item/%E5%B9%BF%E5%9F%9F%E7%BD%91)，有效控制无线网络内用户的上网权限。您可以利用按钮添加新条目来增加新的过滤规则；或者通过“编辑”、“删除”链接来编辑或删除旧的过滤规则。

MAC地址过滤功能：请在该处选择是否开启路由器的无线网络MAC地址过滤功能。

过滤规则：请选择MAC地址过滤规则，该规则对下面MAC地址条目列表生效。

MAC地址：该项指需要进行访问限制的无线网络内的主机MAC地址。

状态：该项显示MAC地址过滤条目的状态。“生效”表示该设置条目被启用，“失效”表示该设置条目未被启用。

描述：该项显示对主机的简单描述。

添加新条目：单击该项，您可以在随后的界面中添加新的MAC地址过滤条目。

使所有条目生效：单击该按钮，您可以使表中的所有条目生效。

使所有条目失效：单击该按钮，您可以使表中的所有条目失效。

删除所有条目：单击该按钮，您可以删除表中所有的条目。

2. 802 1x端口访问控制技术。

802.1x协议是基于Client/Server的访问控制和认证协议。它可以限制未经授权的用户/设备通过接入端口(access port)访问LAN/WLAN。在获得交换机或LAN提供的各种业务之前，802.1x对连接到交换机端口上的用户/设备进行认证。在认证通过之前，802.1x只允许EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

网络访问技术的核心部分是PAE（端口访问实体）。在访问控制流程中，端口访问实体包含3部分：认证者--对接入的用户/设备进行认证的端口；请求者--被认证的用户/设备；认证服务器--根据认证者的信息，对请求访问网络资源的用户/设备进行实际认证功能的设备。

端口访问控制技术在最开始只是防止非法用户使用网络，用于以太网的认证接入，后来却发现无线网利用这种技术可以有效解决网络安全接入问题。无线工作站STA会在与无线访问点AP关联后向AP发送认证消息，在未被授权以前，即使STA与AP继续关联着，却始终无法访问网络，只能继续发送认证消息知道授权。所以联系无线网的用户是否可以上网则就取决于802.1x 的认证结果。对于公共无线网络接入的安全问题，无线工作站必须安装802.1x 客户端软件，无线AP要内嵌802.1x认证代理，与此同时还需作为Radius 客户端，把用户的认证信息转发给服务器，除上述功能外，它还可以提供用户认证和计费系统。

3.VPN技术

VPN属于远程访问技术，简单地说就是利用公用网络架设专用网络。例如某公司员工出差到外地，他想访问企业内网的服务器资源，这种访问就属于远程访问。

优点

VPN能够让移动员工、远程员工、商务合作伙伴和其他人利用本地可用的高速宽带网连接（如DSL、有线电视或者WiFi网络）连接到企业网络。此外，高速宽带网连接提供一种成本效率高的连接远程办公室的方法。

设计良好的宽带VPN是模块化的和可升级的。VPN能够让应用者使用一种很容易设置的互联网基础设施，让新的用户迅速和轻松地添加到这个网络。这种能力意味着企业不用增加额外的基础设施就可以提供大量的容量和应用。

VPN能提供高水平的安全，使用高级的加密和身份识别协议保护数据避免受到窥探，阻止数据窃贼和其他非授权用户接触这种数据。

完全控制，虚拟专用网使用户可以利用ISP的设施和服务，同时又完全掌握着自己网络的控制权。用户只利用ISP提供的网络资源，对于其它的安全设置、网络管理变化可由自己管理。在企业内部也可以自己建立虚拟专用网。

缺点

企业不能直接控制基于互联网的VPN的可靠性和性能。机构必须依靠提供VPN的互联网服务提供商保证服务的运行。这个因素使企业与互联网服务提供商签署一个服务级协议非常重要，要签署一个保证各种性能指标的协议。

企业创建和部署VPN线路并不容易。这种技术需要高水平地理解网络和安全问题，需要认真的规划和配置。因此，选择互联网服务提供商负责运行VPN的大多数事情是一个好主意。

不同厂商的VPN产品和解决方案总是不兼容的，因为许多厂商不愿意或者不能遵守VPN技术标准。因此，混合使用不同厂商的产品可能会出现技术问题。另一方面，使用一家供应商的设备可能会提高成本。

当使用无线设备时，VPN有安全风险。在接入点之间漫游特别容易出问题。当用户在接入点之间漫游的时候，任何使用高级加密技术的解决方案都可能被攻破。

广泛应用在广域网的VPN技术，也就是虚拟专用网，通常会利用因特网来建立一个临时、安全的连接，利用它可以实现远程用户间的内部网络建立安全的连接，目前也已经大规模的用于无线局域网了。而对于诸如在企业内部对网络安全性要求较高的用户，则可以将VPN技术与802.11技术结合，可以较为理想地解诀安全问题。

那么无线网络的安全漏洞及挑战有些什么呢？

无线网络和有线网络有相似之处,它们都采用OSI分层协议的体系结构,在本节中,每-层都有自己独特的安全挑战和问题,由于不同的层依赖于不同的协议，因而表现出不同的安全漏洞。以下总结了无线攻击可能遇到的安全漏洞及挑战。

（1）物理层攻击

物理层位于最底层,用于指定信号传输的物理特性,无线通信的广播特性使其极易受到窃听和干扰。在无线网络中,只要窃听者位于源节点的传输覆盖区域,会话极有可能被窃听。为保证机密传输,采用加密技术,依靠秘密密钥,以防止窃听攻击拦截数据传输,在这种情况下,即使窃听者窃听到会话，因没有密钥而很难从密文中提取到信息。

此外，在无线网络中的恶意节点可以很容易地干扰正常用户间的通信,这被称为干扰攻击(也称为DoS攻击)，损害合法用户的网络可用性。为此，扩频技术(将信号发射在比原来频带较宽的光谱带宽上)被广泛认可为抵御DoS攻击的有效手段。

（2）MAC层攻击

在MAC层,CSMA/CA ,CDMA,OFDMA智能信道接入控制机制使多个网络节点访问共享介质。通常,每个网络节点配备一个网卡和一个唯一的MAC地址用于用户认证。攻击者试图用恶意更改其分配的MAC地址被称为MAC地址欺骗，这是MAC攻击的主要技术。此外,MAC的攻击者通过窃听网络流量,通过分析听到的流量窃听节点的MAC地址，这称为身份盗窃攻击，攻击者试图通过身份盗窃假装是合法的网络节点，并获得受害者节点的保密信息。

除了上述MAC欺骗和身份盗窃,MAC层的攻击类还包括MITM攻击和网络注入。通常，一个MITM攻击是指攻击者为了拦截一对合法通信节点的MAC地址首先“嗅”网络的通信,然后模拟两个受害者并建立与他们的联系,这样,MITM攻击者作为受害者使他们之间的中继觉得他们之间的沟通与对方直接通过专用连接。在现实中,他们的会话被攻击者截获和控制。相比之下,MITM攻击的目的是防止网络设备的运行,如路由器,交换机等,通过注入伪造的网络重新配置命令,在这种情况下,如果一个压倒性的伪造的网络命令开始,整个网络可能会瘫痪,因此需要重新启动或重新编程的所有网络设备。

（3）网络层的攻击

网络层攻击利用IP层的弱点，即所谓的Smurt 攻击、IP欺骗和劫持。具体说来,IP欺骗是攻击者复用一个伪造的IP地址用于隐藏身份或冒充另个网络节 点进行非法活动。 IP劫持如果攻击者成功劫持到IP地址,就可以断开合法用户重新创建一个网络连接，从而获取机密信息。

Smurf攻击是网络层DoS攻击，使用IP广播地址发送大量的ICMP数据包(个伪造的源IP地址)到-个或组受害节点,收到ICMP请求时,受害者需要发送ICMP应答,增加网络负荷。在Smurt攻击发射数量足够高的ICMP请求时,网络将不堪重负而瘫痪。防御Smut攻击,-个可能的解决方案是确保用户和路由器不会不断回应ICMP请求。我们也可以考虑使用防火墙,它可以拒绝恶意数据包从伪造的源IP地址到达。

（4）传输层的攻击

TCP攻击包括TCP泛洪攻击和序列号预测攻击。TCP泛洪攻击指攻击者发送一个压倒性的ping 请求数，如ICMP回送请求受害者的节点，然后通过发送ping响应回复,，如ICMP回送答复。当ping请求的数量是足够高的,将会延迟受害节点连接至目标网络。TCP序列预测攻击者首先猜测受害者的TCP序列索引,伪造数据包发送给受害者，破坏数据完整性。此外,UDP也容易发生泛洪攻击。

（5）应用层的攻击

应用层支持HTTP的Web服务、FTP文件传输和SMTP邮件传输,这些协议都容易出现安全攻击。例如HTTP是通过网络交换超文本的协议,这是众多的安全威胁,主要包括恶意软件的攻击（例如，木马，病毒，蠕虫，后门程序，键盘记录器等）、结构化查询（SQL）注入攻击和跨站脚本攻击等等。

无线网络有着巨大的发展前景，相应的WIfi安全技术也应提高其发展的速度。如果WiFi安全技术不能随着无线网络的发展而发展，那么用户信息在网络上受到攻击或者丢失都将成为严重的问题。