无线攻击和漏洞

无线攻击和漏洞

目前很多公司都已经配置了企业级别的 802.11 (Wi-Fi)无线局域网。然而，虽然最近技术提高了，但是安全问题依然被认为是首要的挑战。没有充足的安全措施，无线就会为新的攻击开放企业网络。本专题将帮助您理解 Wi-Fi 的技术内在漏洞和对它攻击。

无线攻击和漏洞介绍

现在三分之二的公司已经配置了企业级别的 802.11 (Wi-Fi)无线局域网。然而，虽然最近技术提高了，但是安全问题依然被认为是首要的挑战。没有充足的安全措施，无线就会为新的攻击开放企业网络，这些攻击范围广泛：从驾驶攻击和密码破解，到欺骗和双子星病毒。为了防止无线相容性认证(Wi-Fi)成为你网络防护的软肋，有必要理解无线带来的商业风险、可以减少这些风险的对策、以及设计、配置和监测安全无线局域网的行业最佳方式。

- 无线安全：知识就是力量

无线攻击基本知识

在我们充满专业术语的行业，清除你的周围充满的无线攻击，以及它们潜在的商业影响非常困难。本条技巧中提供了预防对 802.11 和 802.1X 攻击的相关列表，列表中按照威胁的类型分类，并列出了相关的攻击方法和工具，这样我们就理清了混乱无序的情况。

- 无线攻击的基本知识（一）
- 无线攻击的基本知识（二）

无线漏洞评估

严格的定期漏洞评估可以帮助在攻击者发动攻击之前，查找和修复 WLAN 漏洞。但是但是从哪里开始呢？应该查找什么呢？如何涵盖所有的位置呢？在这份清单中，TechTarget 中国的特约专家将帮助你回答这些问题，并提供一个框架，从而开发适合你自己的 WLAN 的漏洞评估程序。

- **Wi-Fi 漏洞评估清单**

无线欺骗性攻击

论你的公司是否运行或禁止的 Wi-Fi，未经授权的“欺骗”访问点或者站点可能已经拜访了你的办公室。大多数 WLAN 的用户将消除欺骗性威胁列为重中之重。虽然监测欺骗性威胁相当容易，但是消除这些欺骗性威胁却是出乎意料的艰难。本文中 TechTarget 中国的特约专家系统地描述了一种捕获欺骗性威胁的过程和工具，从而简化这个问题。

- **捕获欺骗性威胁的秘诀**

无线安全：知识就是力量

根据 2005 年 WLAN 市场情况的调查，现在三分之二的公司已经配置了企业级别的 802.11 (Wi-Fi)无线局域网。然而，虽然最近技术提高了，但是安全问题依然被认为是首要的挑战。

没有充足的安全措施，无线就会为新的攻击开放企业网络，这些攻击范围广泛：从驾驶攻击和密码破解，到欺骗和双子星病毒。为了防止无线相容性认证(Wi-Fi)成为你网络防护的软肋，有必要理解无线带来的商业风险、可以减少这些风险的对策、以及设计、配置和监测安全无线局域网的行业最佳方式。

有风险的企业

人们认为忽视无线威胁不再是一种可行的选择。调查显示现在大部分企业发现不知名的"欺骗"访问点在其设备内部或附近运行。去年，装好的笔记本中五分之四都内置了无线相容性认证(Wi-Fi)，大多数办公室现在也配备有未授权的无线客户机，这些客户机是由客户、供应者、合作伙伴和传递人员携带的。结果，每个企业——包括哪些还没有配置 Wi-Fi 的企业和那些禁止 Wi-Fi 的企业——应当准备好监测活动，并保护企业资源，以防受到以无线为基础的攻击。

没有配置正式无线局域网的企业会面临欺骗性接入点和客户机带来的威胁。比如，粗心的雇员将许多欺骗性接入点安装在企业防火墙内，而没有采用任何安全措施。尽管并非出于恶意，但是，这些接入点在你网络的中心仍然担当未受保护措施的后门，外界可以从这里获得秘密数据和敏感系统。更糟糕的是，笔记本电脑上的小型传播性接入点和易受攻击的接入点也更容易隐藏攻击者的欺骗。在家或热点使用 Wi-Fi 的工作者可能会在办公室无意地重新连接到类似名称的欺骗接入点，在企业网络和攻击者之间创建了一座桥梁。

大部分公司都配置了无线局域网（WLAN），如果你的公司也是其中的一员，那么你就面临着多余的顾虑。主要的顾虑之一就是保护无线资源，防止误用、滥用和攻击。比如，Wi-Fi 就仅会受到一种剩余的新型服务拒绝攻击的攻击，这个攻击利用了 802.11 和 802.1X，以及执行这些协议相对不成熟的产品。在把关键任务系统从有线以太网移动到无线局域网之前，关键是要了解这些服务拒绝风险，以及关于这些风险你所能采取的措施和你不能做的。此外，虽然，我们很容易了解了办公室内部的 Wi-Fi 客户机所面临的威胁，但是我们仍然发现了一些办公室内部的无线所引进的新威胁。简言之，Wi-Fi 创建了混合托管的支网，可以保证仔细的检查、并添加保护层，进一步削弱了已经瓦解的网络外围。

预先警告意味着预先准备

当然，任何网络都有风险。90 年代，在保护我们企业网络不受因特网攻击的同时，我们学会了如何利用环球网的优点。这十年中，在采用安全措施以保持这些风险出于控制之中的同时，我们必须学会选择 Wi-Fi 的金融潜能和生产潜能。

幸运的是，所有新的 Wi-Fi 产品包括数据链接安全特性，该特性能够抵抗诸如有线等效保密(WEP)破解之类的成熟攻击。今天所出售的大部分企业级别的产品，都支持 802.11i Security Enhancements——该性能可以提供强大的数据加密、完整性、用户认证和端口访问控制功能。虽然这些功能提供了一定的保证——真正的、基本的保证——但它们本身并不足以创建一个安全的无线网络。

配置强大的防御系统需要一个策略：明确的安全策略可以鉴别威胁、与企业有关的风险和用于减轻风险的对策。如果你不了解这些无线威胁和攻击方法，那么你就不可能评定它们的潜在企业影响。如果你不了解这些风险，你不能知道哪些策略可以有效地预防风险。你应该执行 WPA-PSK 还是 802.1X？如果是 802.1X，你应该支持哪些 EAP 类型？关于发现并消除欺骗性设备，你的策略是什么？是否有成本效益呢？创建一个无线安全策略，可以帮助你解决诸如此类的问题，以及更多的问题。

如何开始

有很多关于 Wi-Fi 安全方面的信息，此外，还有很多可用的良好资源，可以学到更多这方面的知识。每天负责安全的 WLAN 管理员应当考虑诸如 Planet3 CWSP 项目之类的证书。技术家可以在 CWNP 学习中心找到许多详细的 802.11 安全文件。

然而，许多 IT 专家和网络管理员所面临的挑战正在这一复杂的主题中占有一席之地，从新的挑战中寻找以往的挑战，透过树木发现森林。如果听起来比较熟悉的话，那么请核查我们新的“无线安全午餐学习时间”（Wireless Security Lunchtime Learning）系列。这一系列的 20 分钟网络版策略和双战术技巧是为那些时间有限而又渴求 WLAN 安全知识的读者而设计的。为了看看你从这一系列中学到了些什么，可以参加我们的入门考试（Entrance Exam）。从无线攻击和最佳方式到入侵监测和防御，这一系列技巧会用所需要的基本信息来武装你，这样你可以处理 Wi-Fi 威胁。

（作者：Lisa Phifer 译者：李娜娜 来源：TechTarget 中国）

无线攻击的基本知识（一）

在我们充满专业术语的行业，清除你的周围充满的无线攻击，以及它们潜在的商业影响非常困难。本条技巧中提供了预防对 802.11 和 802.1X 攻击的相关列表，列表中按照威胁的类型分类，并列出了相关的攻击方法和工具，这样我们就理清了混乱无序的情况。

访问控制攻击

这些攻击使用无线或者规避无线局域网访问控制方法，比如 AP MAC 过滤器和 802.1X 端口访问控制，进而试图穿透网络。

攻击类型	说明	方法和工具
驾驶攻击	通过监听信标或者发送探测请求，进而发现无线局域网，从而为进一步的攻击提供登录点。	DStumbler, KisMAC, MacStumbler, NetStumbler, WaveStumbler, Wellenreiter
欺骗性接入点	在防火墙内部安装不安全的接入点，在受信任网络中创建开放后门。	任何硬件或软件接入点
点对点连接	直接连接到不安全的站点，避开安全的接入点，进而攻击站点。	任何的无线网卡或者 USB 适配器
MAC 欺骗	重新配置攻击者的 MAC 地址，伪装成一个授权的接入点或站点。	Bwmachak, changemac.sh, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS 破解	通过来自 802.1X 强制访问请求，恢复 RADIUS 秘密，进而使用 evil twin AP。	位于局域网或者网络中接入点和 RADIUS 服务器之间路径上的信息包捕获工具

机密性攻击

这些攻击试图截取无线组织发送的私人信息，不论是通过 802.11 还是高层协议，以明文还是加密形式发送的信息。

攻击类型	说明	方法和工具
窃听	捕获未受保护的应用层信息流，并对其解码，以获得潜在的敏感信息。	bsd-airtools、Ethereal、Ettercap、Kismet、商业分析器
WEP 密钥破解	使用强力或 Fluhrer-Mantin-Shamir（FMS）密码分析学，来捕获数据，并重现设置 WEP 密钥	Aircrack、AirSnort、chopchop、dwepcrack、WepAttack、WepDecrypt、WepLab
双子星病毒接入点	通过为无线局域网的服务集标识符（SSID）设置信标，吸引用户，伪装成授权的接入点。	cqureAP、HermesAP、HostAP、OpenAP、Quetec、WifiBSD
接入点网络钓鱼攻击	在 evil twin 接入点上运行假冒的入口或者网络服务器，用网络钓鱼的方式引诱用户登录，获得信用卡号码	Airsnarf、Hotspotter
中间人攻击	在 evil twin 病毒接入点上运行传统的中间人攻击工具，截取 TCP 会议或 SSL / SSH 信道。	Dsniff、Ettercap

完整性攻击

这些攻击通过无线发送伪造的控制、管理或者数据帧，误导接受者或者推动其它类型的攻击（比如，拒绝服务攻击）。

攻击类型	说明	方法和工具
802.11 帧注入	编写并发送伪造的 802.11 帧。	Airpwn、File2air、libradiate、void11、WEPWedgie、wnet dinject/reinject
802.11 数据重发	捕获 802.11 数据帧以备后续的（修改）重发。	捕捉工具+注射工具
802.11 数据删除	在欺骗 ACK 的同时，干扰预定的接收器，防止其发送信息，进而删除数据帧。	干扰工具+注射工具
802.1X 扩展认证协议(EAP)重发	捕捉 802.1X 的扩展认证协议（比如，EAP 的身份、成功、失败），进而稍后进行重发。	无线捕获工具+站点和接入点注入工具
802.1X RADIUS 重发	捕捉 RADIUS 的访问-接受或拒绝信息，以备后续的重发。	以太网捕获工具+接入点和认证服务器注射工具

(作者：Lisa Phifer 译者：李娜娜 来源：TechTarget 中国)

无线攻击的基本知识（二）

认证攻击

入侵者使用这些攻击，窃取合法用户的身份和证书，进而访问其它私密网络和服务。

攻击类型	说明	方法和工具
共享密钥猜测	采用猜测、厂商默认或者破解 WEP 密钥，进而实现 802.11 共享密钥猜测。	WEP 破解工具
PSK 破解	使用字典攻击工具，从捕获的密钥同步信息交换帧那里重新获得 WPA PSK	coWPAtty、KisMAC、wpa_crack、wpa-psk-bf
应用层登录窃取	从明文应用协议捕获用户证书（例如，电子邮件地址和密码）。	Ace Password Sniffer、Dsniff、 PHoss、 WinSniffer
域登录破解	使用蛮力攻击工具或者字典攻击工具，破解 NetBIOS 哈希密码，重新获得用户证书（例如，Windows 登录名和密码）。	John the Ripper、LOphtCrack、Cain
VPN 登录破解	在 VPN 认证协议上运行蛮力攻击，获得用户证书（例如，PPTP 的密码或 IPSec 预共享密钥）。	ike_scan and ike_crack (IPsec)、anger and THC-pptp-bruter (PPTP)
802.1X 身份窃取	从明文 802.1X 的身份响应数据包中捕获用户身份。	捕捉工具
802.1X 密码猜测	使用捕获的身份，多次尝试 802.1X 身份验证，进而猜测到用户的密码。	密码字典
802.1X LEAP 破解	使用字典攻击工具破解 NT 密码散列，从捕获的 802.1X LEAP 信息包中，恢复用户证书。	Anwrap、Asleap、 THC-LEAPcracker
802.1X EAP 降级	使用伪造的 EPA-响应/否定应答信息包，迫使 802.1X 服务器提供较弱的认证类型。	File2air、libradiate file2air、libradiate

有效性攻击

这些攻击采用拒绝合法用户的访问无线局域网资源或者削弱那些资源的方法，从而阻止把无线服务传递给合法的用户。

攻击类型	说明	方法和工具
接入点盗窃	从公共空间物理移除接入点。	“Five finger discount”
射频干扰	与目标无线局域网的同一频率进行传递，可能以超过等效全向辐射功率（EIRP）规定的强度进行传递。	射频干扰机、Microwave oven、带有 Alchemy/HyperWRT 固件的接入点
Queensland 服务拒绝攻击	利用载波监听多路访问/冲突防止（CSMA/CA）协议，空闲信道评估机制，来使得信道繁忙。	支持 CW Tx 模式的适配器，可以用低层次效用来调用连续传输。
802.11 信标洪流	产生数以千计的假冒 802.11 信标，使站点很难找到合法的接入点。	欺骗性接入点
802.11 证书/认证洪流	从随机的 MAC 发送伪造的身份验证或证书，以填补目标接入点的关联表。	Airjack、File2air、Macfld、 void11
802.11 TKIP MIC Exploit	产生无效 TKIP 数据，以超过目标接入点的 MIC 错误极限，并暂停无线局域网服务。	File2air、wnet dinject
802.11 权力证明洪流	用伪造的权力证明或者假证书来阻断用户与接入点之间的连接。	Airjack、Omerta、void11
802.1X EAP-Start 洪流	用 EAP-Start 信息，消耗资源或摧毁目标，进而淹没接入点。	QACafe、File2air、libradiate
802.1X EAP-失效	观察一个有效的 802.1X EAP 的交换，然后向站点发送一个伪造的 EAP －失效信息。	QACafe、File2air、libradiate
802.1X EAP-of-Death	发送已知格式错误的 802.X EAP 的身份响应，进而造成一些接入点的破坏。	QACafe、File2air、libradiate
802.1X EAP 长度攻击	用长度错误的字段发送 EAP 具体类型的信息，试图摧毁接入点或者 RADIUS 服务器。	QACaf、File2air、libradiate

注意：许多这些工具都可以在 Auditor Security Collection 中找到，Auditor Security Collection 是一个以 KNOPPIX 为基础的工具包，目的是为了在渗透测试和漏洞评估中使用。

（作者：Lisa Phifer 译者：李娜娜 来源：TechTarget 中国）

Wi-Fi 漏洞评估清单

漏洞评估可以帮助你在攻击者利用前，找到并修复 WLAN 漏洞。但是从哪里开始呢？应该查找什么呢？如何涵盖所有的位置呢？在这份清单中，TechTarget 中国的特约专家将帮助你回答这些问题。

1．发现临近的无线设备

如果你知道有什么设备，就不能评估 WLAN 漏洞。从搜索办公室内外的无线设备开始，创建后续步骤的基础。

- ✓ 那一个通道拥有 2.4 GHz 带宽的活跃流量？
- ✓ 那一个通道拥有 2.4 GHz 带宽的活跃流量？
- ✓ 在这些频段中，有没有非—802.11 界面的资源呢？

对每一个已知的 802.11 访问端点，记录：

- ✓ 媒体访问控制（MAC）地址
- ✓ 扩展服务集标识符（ESSID）
- ✓ 通道
- ✓ 平均/最高信噪比(SNR)

对每一个一发现的 802.11 工作站，记录：

- ✓ MAC 地址
- ✓ 关联 ESSID
- ✓ 关联接入点或者同等的工作站
- ✓ 平均/最高 SNR
- ✓ 如果可见，802.1X 身份

- ✓ 大约位置和可能的持有人

2．调查欺骗性攻击设备

对于非-802.11 的干扰资源（例如，微波炉、蓝牙和无线电话），光谱分析器可以帮助采集资源痕迹。对于 802.11 设备，把调查结果和你已有的详细目录作对比，分离出需要深入调查的未知设备。注意在带宽和通道中查找通常不使用的活动可以帮助你发现试图逃避检测的设备。为了更多地了解如何调查这些“欺骗”设备和他们对你的 WLAN 产生的风险，请阅读相关的技巧《捕获欺骗性威胁的秘诀》。

3．测试你自己的访问端点

下一步，把你的注意力转移到你自己的 WLAN 资源，从向用户发送无线服务的接入点开始。这些接入点位于包含受信合不受信的设备的网络上。同样的，他们也应该通过对面向互联网的边界防火墙和访问路由器的渗透测试。关于每个接入点，你应该回答如下问题：

- ✓ 接入点运行的是最新的固件和安全补丁吗？
- ✓ 出厂默认 ESSID 已经更改了吗？
- ✓ 默认管理员登录/密码已经更改了吗？
- ✓ 管理员密码是不是容易被破解？
- ✓ 有没有强大的认证选择（例如，隐私密钥）？
- ✓ 有没有开放不必要的端口（例如，Telnet、HTTP、SNMP、TFTP）
- ✓ 这些开放端口容易受到攻击吗？
- ✓ 有没有加密管理界面（例如，SSH、HTTPS）？
- ✓ 是否激活了安全警告和日之（例如，系统日志（sylogs）、traps）？
- ✓ 有没有使用过滤器阻止通过接入点传播到有线网络中的未认证的协议（例如 ARP、RIP、SNMP、NetBIOS）？
- ✓ 有没有（使用）过滤器阻止用户到用户的无线？
- ✓ 接入点使用合适的 ESSID 和通道了吗？

- ✓ 安全参数和拒绝策略一致吗？
- ✓ 如果接入点使用 WEP，破解密钥需要多长时间？
- ✓ 接入点发布已知的漏洞初始化厂商（IV）了吗？
- ✓ 如果接入点使用预共享密钥（PSK），容易破解吗？
- ✓ 如果接入点没有使用 WPA2，可以获得 WPA2 更新吗？
- ✓ 接入点可以抵挡模拟 802.11 拒绝服务攻击吗（例如，认证洪流）？

4.测试你自己的工作站

有些工作站在你调查时可能没有活动，所以确保你的资产详细目录上的每一个 802.11-功能设备都检查了，包括笔记本电脑、桌面电脑、PDA、VoIP 手机、打印机、扫描器和耳机或听筒。你可能想要“ping 扫描”无线子网，来确定逃过早期检查的秘密设备的位置。然后，回答关于你的每一个无线工作站的下列问题：

- ✓ 工作站是否运行了最新的操作系统和应用安全补丁？
- ✓ 是否使用了引导程序或者操作系统认证阻止丢失/被窃/无意使用？
- ✓ 目前的杀毒程序和反间谍软件程序运行了吗？
- ✓ 无线界面有没有被个人防火墙保护？
- ✓ 有没有开放不需要的端口（例如 netbios-ns/ssn、 microsoft-ds、 ssdp）？
- ✓ 有没有通往无线的不必要的协议（例如文件/打印机共享）？
- ✓ 有没有把可能的无线入侵（例如，以阻止的会话）计入日志？
- ✓ 无线客户是否和 ANY 网络相关联？ANY 特别吗？
- ✓ 用户自动使用家庭或者热点 SSID 再聚焦了吗？
- ✓ 磁盘上保留了无线用户的信任状（例如，密码）了吗？
- ✓ 工作站扫描了合适的带宽并使用了合适的 ESSID 了吗？
- ✓ 安全参数和定义的策略一致吗？
- ✓ 工作站发布已知的漏洞 IV 了吗？
- ✓ 如果工作站使用 802.1X，它的认证可见吗？
- ✓ 如果使用 802.1X，检查服务器的证书了吗？

- ✓ 如果不使用 WPA2，可以获得 WPA2 更新吗？
- ✓ 如果在无线上使用 VPN 客户端，配置合适吗？

5．测试你的 WLAM 架构

最后，评估无线子网中的所有网络架构设备的安全性，包括无线交换机、防火墙、VPN 网关、DNS 服务器、DHCP 服务器、RADIUS 服务器、运行被俘入口登录页的 Web 服务器和管理以太网的交换机。

和接入点一样，所有的这些设备应该通过相同的通常运行面向互联网的服务器的渗透测试。例如，被俘入口应该通过通常运行 DMZ Web 服务器的测试。包括按照设计评估对需要补丁的已知漏洞的程序/版本的测试。

大部分的架构测试都不是为无线特定的，但是附加的测试可能适合 802.1X 架构。例如，你可能希望测试 RADIUS 服务器的功能来温和的拒绝错误格式的 EAP 信息，包括有害 EAP 长度和深度。

6．采用测试结果

很不幸，没有可以帮助你进行最后的一步的清单。现在应该回顾一下测试结果，并评估你可能没发现的漏洞。排除可能的漏洞，并降低可能利用其他漏洞的机会。例如，如果你在接入点上发现了远程登录，决定是否停止服务，以及如何停止。你可以使用 SSH 代替远程登录来管理接入点吗？你可以把 SSH 限制到以太网上使无线收发邮件的后台程序不被检测到吗？

一旦你使用了修复，重复测试来验证结果是你现在想要的。理想的是，漏洞评估应该定期进行，来检测和评估新的无线设备和配置的更改。还有，寻找可以使测试自动化的机会，让它们更快，更一致、更严格。

（作者：Lisa Phifer 译者：Tina Guo 来源：TechTarget 中国）

捕获欺骗性威胁的秘诀

论你的公司是否运行或禁止的 Wi-Fi，未经授权的“欺骗”访问点或者站点可能已经拜访了你的办公室。大多数 WLAN 的用户将消除欺骗性威胁列为重中之重。虽然监测欺骗性威胁相当容易，但是消除这些欺骗性威胁却是出乎意料的艰难。本文中 TechTarget 中国的特约专家系统地描述了一种捕获欺骗性威胁的过程和工具，可以提供一定的帮助。

处理欺骗风险

发现未授权的接入点（AP）或者站点是非常普遍的，这些所谓的欺骗性威胁可能是来自邻居、销售商、客户、雇员或者恶意攻击者。处理这些欺骗性风险要求识别到信任的设备，这样你就可以减轻他人带来的威胁。由于无线攻击者可以迅速地造成破坏并转移，所以有必要对所有的新设备进行监测，并迅速作出反应。

然而，在大型的无线局域网中有效地处理欺骗性风险也是很重要的。用诸如 NetStumbler 之类的发现工具，对办公室进行抽查，这样需要太长的时间，并且没有作任何评价，也不会包含每个欺骗性威胁的潜在影响。

高效率的风险处理需要用带有无线入侵监测系统（WIDS）的 24x7 无线电进行监测。这可以用无线局域网交换器实现，该交换器可以进行兼职扫描（比如，Airespace 和 Trapeze）；或者用专用的 WIDS 实现，该 WIDS 可以进行全职扫描（比如，AirDefense、AirMagnet、AirTight、Highwall、Network Chemistry）。一个良好的欺骗性工具包应当可以做比发出警报更多的事情——它可以让你有权力调查欺骗性威胁、隔离欺骗性物理地址、以及（在适当的时候）干扰欺骗性通信进行。

为了协助消除欺骗性威胁，你的工具箱也应该包括一个移动的无线局域网分析器。这些分析器可以从大部分 WIDS 经销商、WildPackets、TamoSoft 和 BVS 等的第三方那里购买

到，也可以从诸如 Kismet 和 Ethereal 等开源工具中获得。为了减少站点的压力，可以寻找输入/输出性能，让这些工具与你的 WIDS 共享数据。

消除欺骗性威胁的策略

既然你已经收集了合适的工具，那么接下来就应该制定一套有条不紊的方案来处理欺骗性威胁。这里列出了你的方案中应该包含的一些步骤：

1.创建一个无线设备的基线目录

对现有的 802.11 设备进行调查——接入点、站点和点对点结点——用移动 WLAN 分析器浏览你的站点。每隔一定时间记录样本（例如，在建筑角落的每隔 200 英尺）。合并样本，记录每个设备的 MAC 地址、扩展服务集标识符（ESSID）、平均/峰值信噪比（SNR）、信道、安全状态和 IP 地址。站点可能会使用许多 ESSID 和信道，并依赖与之相关的接入点。为远程邻居建立一个入口，然后使用移动分析器，用你办公室内部和紧邻的足够强大的信号追踪设备。尽力用足够的精度确定可能的拥有者和地址，进而进行分类。

2.对所有发现的设备进行分类，并配置工具

过滤目录，将其分为几个类别，通过不同地处理一些访问控制列表中的设备和安全警报策略，这样你就可以集中精力处理真正的威胁。虽然，你可能会让 WIDS 忽视了远程邻居，但是需要提醒你，注意设备和近邻之间的连接。无论移除还是将其标记为你的官方无线局域网的一部分，消除你办公室内部未经授权的设备。然后创建一个授权的接入点和站点列表，进而执行这些设备的策略。比如，对可能指示偶然重置或者 MAC 欺骗的接入点设置进行监测。现在，准确的分类可以大大节省调查研究的时间。

3. 监控新设备的无线网络和有线网络

安装无线入侵检测系统，可以对你的无线局域网覆盖区进行略微监测，发现邻近或者外部的欺骗性威胁。WIDS 不能监测到的小型或者远程办公室可以用移动分析仪进行随机抽查。如果你拥有无线 IDS/IPS 或者网络管理系统，也可以对它们进行配置，对欺骗性威胁

进行监测——比如，防止未经授权的 MAC 使用你的以太网交换机，或者侦查接入点无线局域网中的意外广播。最后，配置 WIDS 和移动分析仪警报装置，这样你就不会被误报所淹没。举例来说，WIDS 自动对有线交换器的连通性进行跟踪，这样您就可以集中精力处理网络连接的欺骗威胁。

4. 阻止研究调查中的潜在损害

考虑使用 WIDS 的“遏制”功能，自动检测欺骗性威胁或者调查研究后进行手动检测。尽管性能不同，但是通过在欺骗性威胁的 MAC 地址中针对解除认证洪水，接入点或者站点通常可以临时打开你的无线局域网。中止最近的以太网交换端口，通常就可以削弱接入点与网络之间的连接。当你追捕到欺骗性威胁时，虽然遏制功能可以阻止其来带的破坏，但是，它也可能是破坏性的。确保在使用之前，了解清楚这些功能可以干什么——尤其是自动遏制功能。比如，当连接到欺骗性接入点时，你可能很容易就会阻止你的站点。但是，避免阻止欺骗性威胁可能最终来自于你的邻居。

5. 调查新设备，确定威胁

收集证据，弄清楚欺骗性行为是否来自于邻居、访问者、雇员或者攻击者。甚至基本的性能都有帮助，比如 SNR 和 ESSID。如果新的接入点看起来来自于隔壁的咖啡屋，那么打电话过去确认一下。除了连接性追踪，还要使用感应器或者移动分析仪捕获信息流，以确定欺骗性威胁使用的是哪个系统和应用程序。使用定位地图来预测欺骗性威胁的物理地址。虽然性能有所不同，但是，许多 WIDS 可以在平面图上突出显示某个区域，以减少搜索范围到 20 英尺，甚至更少的范围以内。

6. 做出决定，并执行一个永久性措施

使用你调查研究的成果，决定如何永久性处理欺骗性行为。虽然这涉及到政策、策略和进程，但是进行到此为止以及没有关于下一步工作的计划，这些将是毫无意义的。比如，在没有无知的雇员的允许下，你如何消除已经安装好的欺骗性威胁？如果一个恶意的

欺骗性威胁已经留在了办公楼内，你如何保护自己，防止重复的运行该欺骗性威胁呢？如果这个欺骗性威胁是雇员所有的 PDA，你是否有计划进行无线安全使用方面的教育呢？

7. 更新你的设备清单，以反映出结果

你已经采取了永久性措施来消灭欺骗性威胁以后，跟新设备清单以及相关政策，这样将来就可以正确处理设备。如果你在调查期间中止了欺骗性威胁，那么确定现在是否要撤销。如果你不能够发现欺骗性威胁，使用“审查名单”，以在短时间内加快以后的反应或者增强该办公室的监测力度。

（作者：Lisa Phifer 译者：李娜娜 来源：TechTarget 中国）