无线访问安全

无线访问安全

在本专题中，你可以了解无线访问协议的好处与坏处，这样你就可以选择控制、认证和对你的无线局域网的授权访问的最好方式。

无线局域网访问预算

虽然，WPA 和 WPA2-企业提供了功能强大的无线局域网访问控制，但是， 802.1X 具有 IT 员工少，节约财政预算的优点，因而配置 802.1X 对企业而言具有压倒性的吸引力。从外包到开源，再到预共享密码，本文中，Techtarget 中国的特约专家讲述了几个不是很复杂或者花费较少的相关产品。

- **控制无线局域网访问的紧张预算**

选择 802.1X

802.1X 为控制 WLAN 的使用提供可扩展的架构。但是 802.1X 不仅仅是包含几种类型的扩展认证协议（EAP）的封套。在这将近 50 个详细的 EAP 类型中，哪一个在 WLAN 上工作最合适？在本文中，TechTarget 中国的特约专家将把大部分受欢迎的 EAP 类型和 802.1X，以及每个所支持的认证方法、已知的漏洞以及适合的使用环境的做一下比较。

- **选择合适的 802.1X**

无线局域网认证

许多无线局域网的业主都知道 802.1X 使得验证无线用户成为可能。但是你是否知道 802.1X 也可以用于过滤虚拟局域网中的无线信息流，这些信息可以反映出用户和组的许可

呢？本文中，Techtarget 中国的特约专家将探讨如何在认证和授权之间建立这一关键的连接。

- 综合 802.1X 和 VLAN 实现无线局域网认证

无线局域网攻击

Evil Twins 在公共和私人无线局域网中，对于无线用户而言，是一种明显的威胁。在本文中，TechTarget 中国的特约专家描述了保护用户、防御这种了解较少的攻击的步骤。可以学习 SSL 或者 SSH 可能不足以保护用户，以及 802.1X 相互认证如何帮助防御虚假接入点。

- 防御 Evil Twin 攻击

控制无线局域网访问的紧张预算

虽然，WPA 和 WPA2-企业提供了功能强大的无线局域网访问控制，但是， 802.1X 具有 IT 员工少，节约财政预算的优点，因而配置 802.1X 对企业而言具有压倒性的吸引力。从外包到开源，再到预共享密码，本文中，Techtarget 中国的特约专家讲述了几个不是很复杂或者花费较少的相关产品。

外包 802.1X 服务

WPA 和 WPA2-企业使用 802.1X 端口访问控制框架，验证无线用户。在企业网络中一般可以一起找到这个框架与认证服务器，比如 RADIUS 服务器、Windows 活动目录、RSA SecurID 认证管理员和证书颁发机构。有些公司没有认证服务器，并且不愿意安装认证服务器，他们可以将这个组件外包到服务提供。

这些供应商提供管理 Wi-Fi 认证服务。你的接入点可以通过 TLS 信道、跨因特网，将 802.1X/受保护的 EAP 信息转发到供应商的 RADIUS 服务器，而不是咨询你的本地 RADIUS 服务器。在准许或者拒绝访问你的无线局域网之前，这个供应商的 RADIUS 服务器可以验证工作站的身份和密码。通过管理员网络入口，可以在你的帐户中添加或者移除用户名。

这些服务有着本质的不同——比如，McAfee 使用安装好的客户端软件或者客户向导来配置 802.1X 参数，而 Witopia 用安装好的入门指导，就可以自己进行安装。McAfee 用与 WPA-企业版相一致的参数来配置你的接入点，而 Witopia 是由你自己来为 WPA 或者 WPA2-企业配置接入点。无论哪种方法，基本的设置都非常简单。外包 802.1X 服务，你就可以比配置“个人”预共享机密略多一些的精力便可以实现“企业”安全。

有了任何管理服务，那么我们又回到了经费问题上。Witopia SecureMyWiFi 开始就需要一个接入点和五个用户，每年需要 29 美元。为了包括多于五个接入点和 20 个用户（每年 84 美元），需要进行报价。对于一个受保护的网络，小型企业的 McAfee 无线安全每月

开始需要 4.95 美元；对于五个或者五个以上的网络，每月降到了 3.99 美元。通常都会有试用版下载、促销和批量折扣，因此要查看供应商的网站，以了解现在的价格。

构建你自己的 802.1X 基础设施

一些公司宁可拥有他们自己的认证服务器，但是缺少预算来购买商业版的 RADIUS 产品。另一种方法就是考虑使用免费的 RADIUS 服务器，比如 FreeRADIUS 或者 TinyPEAP。但是不要欺骗你自己：配置自己的 RADIUS 服务器需要多余的硬件、技术通、以及至少需要一些辛勤工作。

为了运行 FreeRADIUS，你需要额外的运行 Linux、FreeBSD、OpenBSD、OSF/Unix 或者 Solaris 的时间和服务器硬件。FreeRADIUS 是在 GNU 通用公共许可证下发布的，这就意味着 FreeRADIUS 可以免费下载和安装。当作为无线认证服务器使用时，FreeRADIUS 可以执行 EAP-MD5、EAP-SIM、EAP-TLS、EAP-TTLS、EAP-PEAP 和 LEAP 的访问请求。你可以决定安全策略、服务器配置和用户证书。但是如果你已经付出了努力，你就会拥有一个灵活的 RADIUS 服务器，可以用于其它用途，比如远程用户 VPN 认证。为无线网配置 FreeRADIUS 的相关建议可以立即在这里找到。

另外，TinyPEAP 是一个特殊用途的 RADIUS 执行工具，可以在 Linksys WRT54G/GS 无线路由器或者 Win32 系统上运行。当 TinyPEAP 安装在一个可兼容的 Linksys 路由器上时，它可以格式化厂商的固件，用一个带有非常小的内置服务器创建一个路由器。当 TinyPEAP 安装在 Windows 系统上时，可以创建一个小型的 RADIUS 后台程序，附近的无线路由器可以进行咨询。在这两种情况下，TinyPEAP 都只支持受保护的 EAP 认证，对照用户名和密码的本地列表，检查 802.1X 请求。尽管 TinyPEAP 并不是开放源，但是测试版的二进制文件可以免费下载。

完全跳过 802.1X

一些公司势不可挡的得出了 802.1X 的全部理念，反过来这些公司就可以使用 WPA 或者 WPA2-个人版。当以功能强大的预共享密钥（PSK）为基础时，这些“个人版”的措施仍然代表 WEP 的一种改进。

当预共享密钥（PSK）太短或者由字典中可以找到的单词组成时，很容易就可以猜到这些密钥。攻击者一般需要捕获一些合法用户在连接到无线局域网时交换的信息包，然后运行一个字典式攻击工具，比如 CoWPAtty。为了预防这种攻击，选择一个 PSK 值，这个值至少是 20 个随机的字母数字字符。为了获得最佳效果，使用一个随机密码发生器，并且确保包括数字和混合的密码（比如，T2adREfasACach64a6Us）。

不论你的 PSK 多么的随机或者有多长，每个连接到你无线局域网中的用户必须知道这个密码，或者将其配置到其系统中。设定好的密码可以使得生活更便捷，因为他们无需记住或者正确地输入一长串的随机字符。但是如果一些人丢失了笔记本或者置之于无人看管时，这个设定好的密码就会受到威胁。另一方面，提示输入 PSK 增加了如下情况发生的机率：用户将密码告知客户、将密码写在便签上或者偷漏整个无线局域网的密码。

虽然，定期更新你的无限局域网 PSK 可以减少风险，但是，组密码最终只可以到此为止。如果你的公司真正在乎如何使外界无法进入你的无限局域网——或者及时了解什么人在任何端点正在使用你的无线局域网——那么，升级到 WPA 或者 WPA2-企业版。

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

选择合适的 802.1X

802.1X 为控制 WLAN 的使用提供可扩展的架构。但是 802.1X 不仅仅是包含几种类型的扩展认证协议（EAP）的封套。在这将近 50 个详细的 EAP 类型中，哪一个在 WLAN 上工作最合适？在本文中，TechTarget 中国的特约专家将把大部分受欢迎的 EAP 类型和 802.1X，以及每个所支持的认证方法、已知的漏洞以及适合的使用环境的做一下比较。

EAP-MD5 (Message Digest #5)

LEAP (轻量级 EAP， Lightweight EAP)

EAP-TLS (传输层安全，Transport Layer Security)

EAP-TTLS ((隧道 TLS ，Tunneled TLS)

PEAP (受保护的 EAP， Protected EAP)

EAP-MSCHAPv2 (Microsoft Challenge 握手协议，Microsoft Challenge Handshake Protocol)

EAP-GTC ((一 般标记卡，Generic Token Card)

EAP-SIM (用户识别，Subscriber Identity Module)

EAP-AKA (Authentication and Key Agreement)

EAP-FAST (Flexible Authentication via Secure Tunneling)

Wi-Fi Alliance Certification

EAP-MD5 (Message Digest #5)

EAP-MD5 (Message Digest #5)

这种 EAP 类型提供了单向客户认证。服务器向客户发送随机问题。客户通过使用 MD5 列出问题和它的。因为人在中间的攻击可以看到问题和回应，EAP-MD5 在开放的媒体上使用时，很容易受到字典式攻击。因为没有服务器认证，它也很容易受到欺骗攻击。最后，EAP-MD5 不可以发送密钥。结果，EAP-MD5 可能用于以太网上，但是永远也不能用到无线局域网上。

LEAP（轻量级 EAP）

也叫做 EAP-Cisco Wireless。这种 EAP 类型在 Cisco 无线局域网上提供了客户端和服务器的相互认证。和 EAP-MD5 一样，轻量级的服务器向客户端发送随机问题，客户会返回一个哈希密码。认证的客户会向服务器发出问题，需要密码，接着是密钥交换。因为 LEAP 是所有权协议，它只能和思科接入点和思科的兼容卡一起用于企业无线局域网。目前，有很多攻击工具可以用于破解 LEAP 认证密码。因此，新的无线局域网应该避免 LEAP。如果你的无线局域网已经使用了 LEAP，确保每一个客户端和服务器使用较长的随机密码，并且尽快更新到更强大的 EAP 类型。

EAP-TLS（传输层安全）

这种 EAP 类型通常被认为是现有的最强大的、配置最广泛的。它使用标准的 TLS 协议（用于保护大部分 Web 传输的 SSL 协议的子协议）在客户端和服务器提供手动认证证明。这个服务器使用 TLS 证明它持有数字证书，向客户端的请求是一样的。客户端使用它的证书证明他的身份，发送的材料也是互换的。一旦认证完成，TLS 通道就终止了，但是 EAP-TLS 发送的密钥可以用于加密 AES、TKIP 或者 WEP 数据。EAP-TLS 在 WLAN 中很合适，在

WLAN 中，客户端已经有了数字证书或者在这里，需要再公共密钥架构中投入高度的安全，来管理这些证书。

EAP-TTLS（隧道 TLS）

EAP 类型通过在客户端放置合法密码认证方法的证书，在安全和配置成本之间平衡，这些合法密码的认证方法例如 PAP、CHAP、MSCHAPv2。EAP-TTLS 要求服务器通过验证并建立 TLS 隧道来自我认证。通过这些 TLS 隧道对客户端发出挑战。甚至当返回明文密码，客户回应就被模糊了。为了避免暴露客户的名称，EAP-TTLS 应该配置为当启动 802.1X 时，可以发送“匿名”认证，然后通过 TLS 隧道，发送实际认证。但认证完成，并且密钥已经发送时，隧道就终止了。EAP-TTLS 适合于 WLAN，而 WLAN 希望可以以安全的方式，重新使用合法的用户认证数据库（例如，LDAP，Active Directory）。

PEAP（受保护的 EAP）

PEAP 和 EAP-TTLS 很相似，但是使用不同客户认证协议。和 EAP-TTLS 一样，PEAP 使用服务器证书，就是 TLS 隧道提供手动认证，并通过加密的隧道提供客户认证。和 EAP-TTLS，PEAP 要求客户使用另外一种 EAP 类型，例如 EAP-MSCHAPv2 和 EAP-GTC（请看下面）。虽然相同的用户信任状都可以用于 EAP-TTLS，但是 PEAP 认证服务器必须可以分析 EAP-TTLS 和所包含的合法认证协议。

注意：*很重要的一点是，在客户端和服务器上要使用相同版本的 PEAP。PEAPv0/EAP-MSCHAPv2 要求 802.1X supplicant（客户端）软件，包括 Windows XP SP2 和 2000 SP4。PEAPv1/EAP-GTC 要求另外的 802.1X supplicant，例如和思科的 Aironet Client Utility 一起安装的那一种。这些 supplicant 是互相排斥的——安装一个 PEAPv1 客户端要替换已经存在的 PEAPv0 的客户端。*

EAP-MSCHAPv2（Microsoft Challenge 握手协议）

这种 EAP 类型可以用于在 TLS 隧道，而 TLS 隧道是由受保护的 EAP 创建的。EAP-MSCHAPv2 在扩展认证协议包装 Microsoft Challenge 握手协议。它适合于那些想要重新使用无线认证的微软用户信任状和服务器（例如，NT 域名控制器和 Windows Active Directories）的公司。EAP-TTLS/MSCHAPv2 也可以完成相同的目标。

EAP-GTC（一般标记卡）

这种 EAP 类型可以用于由受保护的 EAP 创建的 TLS 的内部。EAP-GTC 决定 EAP 的外封带有“旧有密码”，这个密码是由 RSA SecurID 等可携带卡产生的。它适合于使用双因素认证来避免通常的密码攻击（例如，与人共享的密码、写在便笺纸上的密码、存储在被盗笔记本上的密码）的公司——特别是在这些可携带密码已经被远程访问 VPN 使用的公司。这些从混乱中开始的 WLAN 必须决定可携带配制的成本是否合理。

EAP-SIM（用户识别）

这种 EAP 类型提供了手动认证，这是基于 GSM 载体出售的移动电话中发现的 SIM 卡的。SIM 卡可能是插入到双模式的手机中的薄片。执行认证算法的智能卡通常是手机等装置用于认证 GSM 电话网络的。要求携带 EAP-SIM 的 802.11X 是依赖于载体的上通向 GSM 认证服务器的网关的。这种 EAP 类型可以用于智能手机等认证设备，这些智能手机在商用 802.11X 热点和 GSM 网络之间进行信息往来的。

EAP-AKA（认证和密钥协议）

EAp-AKA 和 EAp-SIM 类似，但是可以通过使用用户服务认证模式（USIM）满足非 GSM 载体，而 USIM 是全球移动电讯系统（UMIS）网络上是用的。通过你的载体的网络决定智能手机必须使用的类型，而且 EAP-AKA 使用的永久认证密钥被认为是比 EAP-SIM 使用的导出认证密钥更加强大。

EAP-FAST（通过安全隧道的灵活认证）

这种 EAP 类型是由思科创建的，它是 LEAP 的一种替代类型。 它存在于在先在德思科的接入点和思科兼容无线网卡中。和 PEAP 和 EAP-TTLS 一样，FAST 提供 了隧道手动认证。尽管如此，EAP-FAST 并不要求服务器对自己景象数字认证。与之相反，原来供应的交换创建了共享的秘密，就在受保护的访问信任状（PAC）蜜月。这种 PAC 密钥可以用于所有的后发认证。EAP-FAST 可以满足小型的指纹客户，例如 VoWiFi 手机，它很显然是被数字认证特征查证减缓的。目前，EAP-FAST 仅限于用于基于思科的无线局域网。

Wi-Fi 联合证书

Wi-Fi 联合证书目前可以测试以下的 EAP 类型：EAP-TLS、EAP-TTLS、PEAPv0、PEAPv1 和 EAP-SIM。为了确定你的产品支持哪种类型的 EAP，可以查看 Wi-Fi 联合证书的鉴定产品页。没有经过鉴定的产品可能仍然是，但是在多厂商的无线局域网上配置 802.1X 时，明智的做法是要检查 EAP 类型的兼容性。

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

综合 802.1X 和 VLAN 实现无线局域网认证

许多无线局域网的业主都知道 802.1X 使得验证无线用户成为可能。但是你是否知道 802.1X 也可以用于过滤虚拟局域网中的无线信息流，这些信息可以反映出用户和组的许可呢？本文中，Techtarget 中国的特约专家将探讨如何在认证和授权之间建立这一关键的连接。

标记无线信息流

正如在“使用虚拟局域网（VLAN）分隔无线局域网（WLAN）信息流”技巧中所提到的，使用 802.1Q 标记可以将以太网信息包分割为逻辑组。信息包进入局域网时，可以被标记，这样上游的设备（比如，网关、路由器、防火墙）可以应用安全过滤器和服务质量过滤器。比如，接入点可以标记无线信息流，这样就可以在通过网络，从接入点到边缘交换器、核心交换器、再到因特网路由器时，保证无线信息流与有线信息流分割开来。

在前面的技巧中，我们讨论了有线设备如何使用并过滤标记，以及与虚拟局域网配置有关的最佳方式。但是，你的接入点怎么可以决定哪个虚拟局域网标签可以应用到哪些信息包中？

为了将相同的安全和服务质量策略应用到通过无线进入网络的所有信息流，可以配置你所有的接入点或者边缘交换器，进而分配某个单一的标签。这种方式仅适用于小型、特殊用途特的无线局域网，比如游客因特网访问无线局域网。

配置所有的接入点，进而使 SSID 与独特的虚拟局域网标签（比如，所有从工作站连接到 SSID“员工”到达的信息包会接收到标签#1；而从 SSID“管理员”到达的信息包会接收标签#2）一一对应。这种方法虽然很普遍，但是很容易受到虚拟局域网跳跃攻击的威胁。在本例中，通过连接到“管理员”SSID，用户可以规避与虚拟局域网#1 相关的过滤器，并将其放置于虚拟局域网 #2。

为了防止虚拟局域网跳跃攻击，让你的 802.1X RADIUS 服务器为每个经过验证的用户返回一个许可的 SSID 列表。比如，当 Joe Admin 验证使用 802.1X 时，接收访问信息就可以携带一些标志，允许其使用“员工”或者“管理员”的 SSID。但是，当 Jane Doe 尝试使用“管理员”SSID 时，接收信息提示仅允许她使用“员工”的 SSID。在她发送任何数据之前，Jane 先前所连接到的接入点会与她断开。虽然这种方法支持具有相同认证程度的静态虚拟局域网，但是却具有更强大的访问控制。

为了将你现有的有线网络虚拟局域网应用到与无线网络相连接的站点，必须以用户或者组身份为基础，动态地应用标签。让你的 802.1X RADIUS 服务器为每个经过成功认证的用户返回一个标签，这样就可以实现动态地应用标签的目的。比如，假设你的有线网络分割为有组织的虚拟局域网——标签为#1，用于管理部；标签为#2，用于会计部；标签为#3，用于工程部；标签为#4，用于人力资源部。以太网交换器和防火墙过滤器已经存在，以阻止工程信息流到达会计的数据库。为了将这些控件扩展到与无线网连接的用户，可以配置你的 RADIUS 服务器，只要有来自工程部认证的人通过了 802.1X，都使 RADIUS 服务器返回标签#3。诸如此类等等。这种方法在你的 RADIUS 服务器中集中了虚拟局域网的分配，而不是要求标签配置到每个接入点中。它减少了管理方面的辛苦和错误，并且使你可以消除 SSID 和标签之间的相互影响，这样你可以希望将 SSID 用于另一个用途（比如，WPA2 的转移）。

如何使用 RADIUS 实现虚拟局域网的分配

RFC 3580 详细说明了使用带有远端用户拨号认证服务（RADIUS）的 802.1X 的准则。这些准则解释了如何把 RADIUS 的特性与 802.1X 协议的相应领域相对应起来，包括终止原因、工作站和接入点的验证、超时设定和经销商的特殊属性。特别是，RFC 3580 还讲述了 RADIUS 服务器如何可以使用下面的通道属性，进而在接收访问的信息中返回虚拟局域网标签，这里，虚拟局域网标识符（VLANID）是 1 到 4094 之间的一个整数，编码为一个字符串：

信道-类型= VLAN (13)

信道-媒介-类型=802

信道-个人-组-ID= VLANID

你的 RADIUS 服务器和所有的接入点必须要么支持这个符合 RFC 定义的映射，要么支持专有经销商相同的特殊属性。

你必须配置你的接入点，使其可以从 RADIUS 服务器中接收虚拟局域网的标签值，并将该标签值应用到信息流中，才可以使用这种方法。由你的接入点而定，这可能通过可以应用到单个无线电接收装置或者 SSID 的全程接入点参数或者“RADIUS 概况”而实现。比如，你可以使用 WPA 或者 WPA2-企业版，将一个 RADIUS 概况应用到所有的 SSID 中，而将静态的虚拟局域网标签应用到其它不使用 802.1X 的 SSID 中（比如，访客无线局域网）。当配置虚拟局域网时，建议将独立的虚拟局域网用于接入点的管理部门。

你也许要用用户或者组、以及你希望与它们有关系的虚拟局域网标签，来配置你的 RADIUS。这个 RADIUS 服务器可能本身需要咨询另一个认证服务器，比如域控制器，来确定用户证书。举例来说，域控制器可以返回经过认证用户的组联系，这样 RADIUS 服务器将用于发现正确的标签，并作为信道-个人-组-ID 属性传递回到接入点。

此外，也需要具有虚拟局域网性能的上游设备，包括连接到你接入点的以太网交换器、RADIUS 服务器本身、以及可能还需要一个 DHCP 服务器来将 IP 地址分发到无线工作站。接入点和 RADIUS 服务器可以交换未标记的信息包或者（最好）使用它们自己的虚拟局域网。DHCP 服务器必须参与所有的现行虚拟局域网，对来自每个虚拟局域网的工作站的 DHCP 请求作出响应。

最后，不论你是否将你的整个无线局域网与一个虚拟局域网对应，或是通过 802.1X 分配用户到不同的虚拟局域网，仍然需要访问控制列表来加强安全性或者质量服务策略。虚拟局域网标签使得上游设备可以将不同的策略应用到到达相同物理界面（主干）的局域网信息包。但是，定义这些策略，并确定在哪里应用这些策略，仍然取决于你。

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

防御 Evil Twin 攻击

Evil Twins 在公共和私人无线局域网中，对于无线用户而言，是一种明显的威胁。在本文中，TechTarget 中国的特约专家描述了保护用户、防御这种了解较少的攻击的步骤。可以学习 SSL 或者 SSH 可能不足以保护用户，以及 802.1X 相互认证如何帮助防御虚假接入点。

Evil Twins 如何工作

Evil Twins 是一个虚假的无线访问点，可以通过宣传无线局域网或者扩展服务集标识符（SSID），假冒为合法的接入点或者。Evil Twin 可以使用热点追踪器查看常用的扩展服务集标识符，并使用其中之一作为自己的标识符。热点追踪器是一款监控工作站探测器的攻击工具。或者 Evil Twin 可以和家用的 SSIL（例如，linksys）、热点 SSID（例如，Wayport_Access）或者特定公司的无线局域网配置在一起。甚至在无线电台不发送 SSID 的接入点都可以成为目标，只要合法用户可以用 Ethereal、Kismet 或者另一种无线局域网分析器监测到。

为什么使用别人的 SSID 的接入点很危险？无线工作站通常不和具体的接入点连接；他们和拥有制定 SSID 和最好的信号的任何接入点连接。更糟的是，很多工作站都自动的和过去使用的任何 SSID 重新连接。只要在商务用户的旁边放置一个 Evil Twin，就足以欺骗他们的无线设备和虚假的接入点连接。没有耐心等待用户漫游到 Evil Twin 的攻击者可以使用 AirJack 来证明每个人都是有效的，并强制立即进行再连接。

一旦连接了，Evil Twin 可以使用它的优势发动很多种其它攻击。例如，一部笔记本可以运行 HostAP 和 Airsnarf 创建一个 Evil Twin，进而呈现一种虚假的登录页面来收集用户名称、密码或者信用卡号码。任何 Web 请求都可以通过 DNS 欺骗，被转向到本地主机。Airpwn 等工具可以把恶意回应返回给用户，例如包含植入病毒或者特洛伊木马的 Web

页面。当受害者检查电子邮件或者下载文件的时候，Cain 等破解工具可以从通用的应用协议中提取密码。Dsiff 等人在中间（Man-in-the-middle）工具甚至可以通过作为目标服务器，攻击 SSL 或者 SSH，然后把客户的请求转到合法的服务器上。简而言之，Evil Twin 是一个完美的平台，从这里可以对可信任的用户发起攻击。

阻止这些攻击

从让用户了解 Evil Twin 的风险开始。很多用户很容易和任意的接入点连接来获得免费的互联网访问，而不考虑说可能拥有者写接入点或者这些接入点可能如何欺骗他们显示敏感信息。教育用户避免混乱的无线行为——例如，向他们演示如何关闭自动连接和用户非默认家庭无线局域网 SSID。解释为什么他们永远不能盲目地接受 SSH 公共密钥或者 SSL 服务器新人状，并解释这么做可能的后果。

了解情况的用户作出良好选择的可能性很大，但是任何公司都不能信赖行为端正的用户。向你的用户提供工具，可以监测——或者更好，防御——未授权无线连接。例如：

- 使用无线入侵检测来辨认或者阻止缺乏策略的联合。Network WIDS products 可以为内部无线局域网提供这些服务。主机常驻代理可以把 WIDS 扩展到你自己的无线局域网之外，监控在家里或在路上连接到无限的用户。例如，查看 AirDefense Personal 和 RFprotect Endpoint。
- 中央管理的无线设备配置来避免错误并阻止用户增加不安全的无线网络。例如，Wavelink Avalanche 或者 Windows Active Directory Group Policy Objects 可以用于管理 WinsowsPC 上的 802.11 和 208.1X 参数。
- 为你自己的无线局域网请求 802.1X，使用提供相互认证的 EAP 类型，并总是验证服务器的新人状。虽然这实际上可以证明 RADIUS 服务器的身份，但是服务器证明 RADIUS 机密的接入点的有效性，使 Evil Twin 不能成功地伪装成合法的接入点。
- 向移动工作人员提供安全热点客户端来避免 Web 页面的登录。例如，当连接到“提高的 WPA 网络”时，T-Mobile 的连接管理员使用 EAP-TTLS 的 802.1X。因为

连接管理员自动检查 T-Mobile 服务器的信任状，用户不能以外连接到 Evil Twin，只要用户永远都不接受如何连接到其它 SSID（包括旧的“tmobile” SSID）的选择。

- 最后，教育遥控工作者关于在家庭无线局域网中使用 802.1X 的选择。例如，查看为小企业和 TinyPEAP 的 Witopia SecureMyWiFi、McAfee Wireless Security。

虽然有很多可以用以回避 Evil Twin 的步骤，但是它可能不能排除所有的风险。例如，当在家里工作的时候，你不可能强制用户采用 802.1X 或者当没有 802.1X 支持的时候，你可能需要支持无线设备。为了得到最好的结果，需要把 802.1X 服务器认证和无线客户端监控结合起来。

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