打造安全的无线网络

自无线网络问世以来，它所涉及到的安全问题就成为了公众关注的热点。敏感或机密文件在空中传输，而其内容随时可能被人截获，这另大多数网络管理员感到不安。幸运的是，我们可以使用一些策略来加强无线网络的安全。当你应用了这些技术以后，盗匪组件（Rogue components）就成为了最大的无线安全威胁。

1、不可靠的接入点

2、未授权的接入点

3、恶意的接入点

接下来让我们来深入的了解这三类盗匪接入点，然后我会向你们推荐Kismet，它是一个免费软件，能帮助你追捕盗匪接入点-甚至是那些试图躲避探测的接入点。

不可靠的接入点

你应该提防的第一类盗匪接入点是来自你邻近网络的不可靠接入点。几个月前，一位朋友告诉我这样一件事：他的办公室里并没有无线网络，然而有一天当他将笔记本从家里带到办公室，在公司会议上做陈述的时候，忘记了移除无线网卡。奇怪的事情发生了，他惊异的发现自己的无线网卡自动连接到一个接入点上并被分配了 IP 地址。在客户面前，他假装没有发生任何不寻常的事，但已经迫不及待的要等待会议结束，去调查个究竟了。他很快察出楼下的办公室有一个接入点打开着，并对外分配 IP 地址。

那么来自其他网络的不可靠接入点会给你带来什么样的危害呢？首先，如果你的公司拥有严格的 Internet 访问控制策略而隔壁的公司没有，那么你的雇员也许能够通过一张无线网卡到未授权的站点上尽情的冲浪，而你却永远不会知道发生了什么事。这可能给你的公司带来一些法律上的麻烦（例如，性骚扰诉讼）。

其次，如果你的雇员从邻居的 DCHP 服务器分配到了一个 IP 地址，而这个 IP 地址又正好和本公司另一台客户机一样，则可能会引起网络冲突。换句话说，雇员在连接到本公司的网络做他们应该做的工作的时候，可能会遇到麻烦。

未授权的接入点

你应该提防的第二类盗匪接入点是不怀恶意的员工自行安装的未授权接入点。举个例子来说，去年秋天当我参加 COMDEX 会议的时候，曾和一个因为潜在的安全问题拒绝在其公司部署无线网络的管理人员有过交谈。即使公司并没有无线网络，一个拥有家庭无线网络的员工仍希望在工作地点也炮制一个。因为 IT 部门拒绝安装无线网络，这名员工花了 100 美元购买了一个接入点并将其连如公司的网络（使用公司的以太网插孔），这样他便可以在公司无线使用自己的笔记本。问题出在这名员工知道如何安装无线网络，却不会实现必要的安全规则。这样就可能导致不必要的后果。

恶意的接入点

你应该提防的第三类盗匪接入点是怀有恶意的人连接到你网络的接入点。一般而言，当一个雇员想要嗅探数据包，或者想要将公司的资源泄露出去（对方可能正坐在楼下停车场的汽车中），他将会使用这样的技术。这名员工还将费尽心

机地采取一些措施以让自己的行动更加隐蔽，例如配置盗匪接入点使用隐藏的 SSID。

与盗匪接入点做斗争盗匪接入点可能会给你的网络带来一些严重的问题。很久以前我就已经推荐使用 NetStumbler 来鉴别无线接入点。不过 NetStumbler 只能在 Windows 客户机上工作，而且它提供的检测到的设备信息相当有限。

另一个可选择的解决方案是使用 Kismet。如果说 NetStumbler 只是简单的检测无线网络，那么 Kisme 则的的确确是一个无线网络嗅探器。Kismet 依赖无线网卡的能力来报告数据包。幸运的是，大多数常见的无线网卡-包括 Linksys，D-Link，Cisco Aironet 和 Orinoco-都支持这一功能。你可以在 Linux，BSD 平台上或者在 Windows 平台上借助 Cygwin 的帮助安装 Kismet。

使用 Kismet

Kismet 几乎拥有所有你期待的一个正式数据包过滤工具上出现的所有功能，而它还拥有专门为无线网络量身定做的功能。例如，Kismet 拥有一个内建的机制，来检测任何运行 NetStumbler 的主机。这个软件同样被设计用来解码俘获的数据包。在前面，我提到有些雇员可能会通过隐藏接入点的 SSID 来隐藏盗匪接入点。Kismet 能防止这类技术，因为它支持 SSID 解码。

就像你看到的那样，Kismet 完全有能力在你的网络中检测到盗匪接入点。现在你可能对它的工作方式有一些好奇。Kismet 使用有无线网卡的笔记本或便携机来扫描无线电波。Kismet 可以同时检测到多个源数据包。因为它能够扫描电波，它能在任何可用的频率下检测无线设备。不过，还是有一些检测的限制。当前版本的 Kismet 只能检测 802.11b 的无线设备。如果 802.11g 设备能向下

兼容 802.11b，那么 Kismet 也能检测得到。不过你可以完全忘记使用 Kismet 来检测不流行的 802.11a 网络，除非你找到兼容 Kismet 的 802.11a 网卡。

当 Kismet 检测到设备的时候，它在一张地图上绘制设备的方位。绘图功能可以通过使用可选的 GPS 卡来实现。当无线设备被检测的时候，辨识信息也同样被纪录下来。例如，SSID 将会被纪录下来，因为它是设备的生产商。Kismet 还能够提示你哪些设备使用脆弱的加密，哪些接入点使用缺省的设置（这明显是一个极大的安全风险）。

为了完成绘图，你必须带着运行 Kismet 的无线设备绕着办公室走上一圈，并让 Kismet 看到所有它能检测到的。在绘制每一个检测到的设备的方位时，Kismet 能在地图上绘制圆圈来指示每个设备的信号区域。Kismet 甚至可以推测哪些信号在你没有扫描的区域中是可用的，不过如果条件允许，我还是建议你扫描整栋建筑。

当你完成了无线扫描，分析你搜集到的数据，寻找所有潜在的安全问题或外来的无线设备是至关重要的。如果扫描显示正常，你可以将结果作为今后扫描的基线。当将来你对检测结果不确定的时候，你可以将其与基线扫描相比较，从而判断设备是友好的还是恶意的。

Kismet 最初是设计运行在 Linux 平台上的，如果你必须在 Windows 平台上运行 Kismet，也没有任何问题，你可以安装 Cygwin 并在 Cygwin 环境下运行 Kismet。同样地，还有针对 PDA 的版本，例如使用 Intel Strong Arm 处理器的 iPaqs。你可以在苹果的 OSX 下编译 Kismet，但是当前仅仅只有客户组件是可用的。

盗匪组件是指那些未授权的无线组件。我们讨论得最多的盗匪组件是盗匪接入点，下面是主要的三种形式：