 本周的RSA 2010安全会议提醒人们解决多层面的信息安全问题就好像是一个无休止的打地鼠(whac-a-mole)游戏。一个正在进行的争论是有线网络极好的安全措施是否可以消除扫描附加在有线网络上进行非授权活动的Wi-Fi网络的需求。 在过去的几年里，我听到许多有关这个影响的评论。我在这里简单介绍三个评论： 1.“ 如果我的有线网络是严格封闭的，无线入侵者就不能侵入网络。 ”这看起来似乎是合乎逻辑的，有线安全做得好应该足以保护你的有线数据中心资源。然而，在这个理论中有一些漏洞。第一，黑客很容易引诱你的Wi-Fi用户与他的接入点关联起来、获得那个用户的证书并且以后登录你的有线网络，不用第一次接触那个有线网络。 第二，大多数笔记本电脑和智能手机有Wi-Fi连接和硬盘存储。这些设备可以收发保密的信息并且存储这些信息。因此，Wi-Fi空域和Wi-Fi设备中有数据，而不是在你的有线网络中。这些数据也会发送给入侵者。 最后，仅解决有线网络的安全还不能解决内部员工和承包商的威胁。绕过传统的有线防火墙、AAA服务器和安全网关的最简单的方法是附近的Wi-Fi热点和通过那个连接发送非授权的信息。 2.“ 不会有太多的人把自己的Wi-Fi接入点带到工作站引起风险。 ”这似乎是一厢情愿的想法。IT的日益消费化表明情况正好相反。用户(特别是从幼年开始就习惯于在日常生活中使用IT的年轻人)将利用他们能够利用的任何设备使工作更简单。你可以在你的机构中制定“ 不允许使用无线 ”的政

策，但是，任何人都可以在自己的桌面的以太网接口上插入一个低端的接入点。除非你扫描这个无线电波并且发现这个接入点，否则，你不会知道这个连接。 3.“ Wi-Fi安全公司幻想的流氓Wi-Fi设备的概念就是让我们购买我们不需要的产品。 ”据我看来，你用这个方法抗议有些过分了。这种清理是真实的，每一个机构必须要权衡其安全投资和努力与数据遭到突破可能造成的损失成本，包括硬成本和软成本。但是，连接到你的有线网络或者无线网络信息的非授权的设备确实是流氓设备(或者叫做风险、坏蛋、威胁，你叫什么都可以)。这种设备不应该放在“ 我不会发生这种事 ”的类别中。