Windows XP 无线网络安全精解

早期无线网络由于自身的特殊性和设备昂贵的原因，一直没有普遍开来，因此，无线的网络安全一直也没有引起多少人的注意，随着近几年，无线网络设备的价格一降再降，终于降到了大多数人可以接受的地步，而配置一个无线的网络也不需要具备以往的高级工程师技术，在 Win XP 下，只需要按照向导点击几下鼠标，用不了几分钟就可以建成一个无线网络，简易就是不安全的代名词，因此，无线网络的安全也越来越被人们所关注。

目前无线网络的主要风险体现在服务盗用、数据盗取，数据破坏、干扰正常服务几个方面，这些在 XP 的无线网络里同样存在。为避免安全风险的威胁，我们将逐一进行分析。

还是应了上面的那句话："简易就是不安全的代名词"，XP 的无线安全风险的最大因素，恰恰是来自于 XP 最简单易用的功能——"无线零配置"(WIRELESS? ZERO? CONFIGURATION)，由于接入点可以自动发送接收信号，因此 XP 客户端一旦进入了无线网络信号的覆盖范围，就可以自动建立连接，如果进入了多个无线网络的信号覆盖范围，系统能自动与最近的接入点联系，并自动配置网卡进行连接，完成后，在"可用网络"中将出现建立的连接的 SSID，由于不少厂商使用网卡的半个 MAC 地址来默认命名 SSID，因此，使得 SSID 默认名可以推测，攻击者知道了默认名称后，至少连到接入点的网络是轻而易举了。

主要的针对措施有三个：

1.启用无线设备的不广播功能，不进行 SSID 的扩散

这个功能需要在硬件设备的选项里寻找，启用后将封闭网络，这个时候想连接网络的人必须提供准确的网络名，而不是 XP 系统自动提供的网络名。

2.使用不规则网络名，禁止使用默认名

如果不广播了，攻击者还是可以通过猜测网络名连入网络，因此有必要修改默认名。这里的不规则可以借鉴一下密码设置技巧，不设置具有敏感信息的网络名。

3.客户端 MAC 地址过滤

设定只有具有指定的 MAC 的客户端才可以连接接入点，可以将连入者进一步把关。上面的三个办法只是属于 XP 无线安全的初级设置，不要指望设置了这三个步骤后就可以高枕无忧了，从目前的安全设置来看，虽然可以防备部分无线攻击了，但是，由于并没有对传输中的数据采取任何加密措施，因此，只要攻击者使用一些特定的无线局域网工具，就可以抓取空中的各种数据包，通过对这些数据包的内容分析，可以获得各种信息，其中就包括 SSID 和 MAC 地址，因此前面的三个办法对于这种攻击就形同虚设了。我们下一步面临的是无线传输的加密问题----WEP。