网络安全知识普及无线路由器

1. AP Isolation(AP 隔离)

在很多文章里，我们都能看到这种解决无线安全的方法，相对来说，这是较简单的一种。它类似于有线网络的 VLAN，将所有的无线客户端设备完全隔离，使之只能访问 AP 连接的固定网络，相当于无线中的局域网。

一些大型的公共场所，如机场、酒店等可以采用这个方法来完成公共热点 Hot Spot 的架设，它可以让接入的无线客户端保持隔离，保证旅客们之间的距离，提供安全的 Internet 接入。

2. MAC 过滤

这种方式就是通过对 AP 的设定 ,将指定的无线网卡物理地址输入到 AP 中。而 AP 对收到的每个数据包都会做出判断，只有符合设定标准的才能被转发，否则将会被丢弃。这种方法尽管简单，但安全性其实很差。

3. 隐藏 SSID

什么是 SSID 号?SSID(Service Set Identifier)也可以写为 ESSID ,用来区分不同的网络，最多可以有 32 个字符，无线网卡设置了不同的 SSID 就可以进入不同网络，SSID 通 常由 AP 或无线路由器广播出来，通过 XP 自带的扫描功能可以相看当前区域内的 SSID。出于安全考虑可以不广播 SSID，此时用户就要手工设置 SSID 才 能进入相应的网络。简单说，SSID 就是一个局域网的名称，只有设置为名称相同 SSID 的值的电脑才能互相通信。

SSID 参数在设备缺省设定中是被 AP 无线接入点广播出去的，客户端只有收到这个参数或者手动设定与 AP 相同的 SSID 才能连接到无线网络。如果把这个广播禁止，一般的漫游用户在无法找到 SSID 的情况下是无法连接到网络的。

不过有一种叫做 sniffer 的软件可以将网卡接收到的数据包进行记录，这些数据包中有很多是这个网卡需要接收的信息，也有很多是广播包或组播包这些 本来应该丢弃的数据包，不管网卡该不该接收这些数据，一旦在上面绑定了 sniffer 就将“忠于职守”地记录这些数据，将这些数据信息保存到 sniffer 程序中。因此无线网络同样可以通过安装无线 sniffer 绑定到无线网卡上，从而实现对 SSID 号的察觉与发现。

4. WEP 加密

WEP 是 Wired Equivalent Privacy 的简称，所有经过 Wi-Fi 认证的设备都支持该安全协定，是无线设备中最基础的加密措施，很多用户都是通过它来配置提高无线设备的安全，采 用 64 位或 128 位加密密钥的 RC4 加密算法，保证传输数据不会以明文方式被截获。

它其实是 802.11b 标准里定义的一个用于无线局域网(WLAN)的安全性协议，被用来提供和有线 LAN 同级的安全性。LAN 天生比 WLAN 安全，因为 LAN 的物理结构对其有所保护，部分或全部网络埋在建筑物里面也可以防止未授权的访问。

而经由无线电波的 WLAN 没有同样的物理结构，因此容易受到攻击、干扰。WEP 的目标就是通过对无线电波里的数据加密提供安全性，如同端-端发送一 样。WEP 特性里使用了 rsa 数据安全性公司开发的 rc4 prng 算法。如果你的无线基

站支持 MAC 过滤，推荐连同 WEP 一起使用这个特性(MAC 过滤比加密安全得多)。

该方法需要在每套移动设备和 AP 上配置密码，部署比较麻烦。

不过它的安全性早就不再受到欢迎 ,网上有很多关于破解 WEP 密码的文章，步骤详细，随随便便找一篇就可以轻松搞定。此方法仅能用于确信自己不会被攻击的用户。

5. WPA 加密

WPA 加密即 Wi-Fi Protected Access，其加密特性决定了它比 WEP 更难以入侵，所以如果对数据安全性有很高要求，那就必须选用 WPA 加密方式(Windows XP SP2 已经支持 WPA 加密方式)。

就家庭用户而言，这个方法目前最好的无线安全加密系统，WPA 率先使用 802.11i 中的加密技术 TKIP(Temporal Key Integrity Protocol)。

6. TKIP

新一代的加密技术 TKIP 与 WEP 一样基于 RC4 加密算法 ,且对现有的 WEP 进行了改进，在现有的 WEP 加密引擎中追加了“密钥细分(每发一个包重新 生成一个新的密钥)”、“消息完整性检查(MIC)”、“具有序列功能的初始向量”和“密钥生成和定期更新功能”等 4 种算法 ,极大地提高了加密安全强度。TKIP 与当前 WiFiTM 产品向后兼容，而且可以通过软件进行升级，AboveCable 无线产品完全支持 WiFiTM 标准 ,只需要简单的软件升级就可 以实现对 TKIP 的支持。

WPA 的功能是替代现行的 WEP 协议，是改进 WEP 所使用密钥的安全性的协议和算法。它改变了密钥生成方式，加强了生成加密密钥的算法，更频繁地变换 密钥来获得安全;还增加了消息完整性检查功能来防止数据包伪造。因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。WPA 还追加了防止数 据中途被篡改的功能和认证功能。由于具备这些功能，WEP 中此前倍受指责的缺点得以全部解决。

完整的 WPA 实现比较复杂，由于操作过程比较困难，所以在家庭网络中普遍采用的是 WPA 的简化版￣WPA-PSK(预共享密钥)，在 AP(或者无线路由器)以及连接无线网络的无线终端上输入共享密钥来保护无线链路的通信安全。

但是对于企业和政府来说，很多设备和客户端并不支持 WPA，最重要的是 TKIP 加密并不能满足一些更高要求的加密需求，还需要更高的加密方式。

7. WPA2 与 AES 加密

WPA2是Wi-Fi联盟发布的第二代WPA标准。WPA2与后来发布的802.11i具有类似的特性，它们最重要的共性是预验证，即在用户对延迟毫无察觉的情况下实现安全快速漫游，同时采用 CCMP 加密包来替代 TKIP。

8. AES

诞生于 2002 年的 AES 是一种可用来保护电子数据的新型加密算法。特别是，AES 是可以使用 128、192 和 256 位密钥的迭代式对称密钥块密码，并且可以对 128 位(16 个字节)的数据块进行加密和解密。与使用密钥对的公钥密码不同的是，对称密钥密码使用同一个密钥来对数据进行加密和解密。

AES 到底有多安全?这是一个难以回答的问题，但是现在人们一般认为，它是现有的最安全的加密算法。到目前为止，AES 比任何其他加密算法经过了更多 的审查。攻击 AES 的唯一有效方法就是通过强力生成所有可能的密钥，就这一点来说，无论是在理论上和还是在实践上，AES 都被认为是“安全的”。对于 256 位的密钥大小，在一定的时间(在现有的最快系统上甚至需要数年)内，任何已知的强力攻击都无法破坏 AES。

一般家庭用户的无线环境比较纯净，虽然有少许危险，但只要稍加注意，使用更高位的加密方式，定期更改密码，则多半不会遇到外来危险;而企业用户则比较麻烦，建议采用 WPA2 安全加密方案，保证目前最好的加密效果。

最后需要说明的是 :各种安全方案和加密方式必须是无线路由器(AP)和客户端(计算机的无线网卡)必须同时支持;并且越高级的加密算法对客户端(包括无线路由器和计算机)的运算能力要求越高，也就是说你的计算机 CPU 占用率会更高，网络传输效率会更低。