WI-FI 无线数据分析

WI-FI（Wireless Fidelity）无线数据传输，目前使用已经非常普及，特别是最近这几年智能手机以及平板电脑的发展，WI-FI 已成为这些移动设备的标配。我们在日常生活当中享受这些智能设备为我们带来方便的同时，有没有想过它同时可能会使我们的之间传输的数据遭到窃听，甚至篡改呢？

通常我们在使用 WI-FI 上网时，需要先连接一个 AP（Access Point）设备，例如在咖啡厅或者家里，开启移动设备的 WI-FI 功能，扫描之后会看到一些 AP 的 SSID（Service Set Identifier）名称（如果该 AP 没有进行广播，那么将扫描不到），只有连接上相应的 AP 之后（如果连接 AP 需要密码，那么必须先输入密码才行），才能通过该 AP 上网。

最初无线数据传输的保密性是通过 WEP 保证的，但是发布之后，被发现有几个严重的弱点容易导致数据被破解。后来才有 Wi-Fi 联盟发布的 IEEE 802.11i 中的 WPA2。

在 WPA2 推出之前，先是有了 WPA。WPA 是一种基于标准的可互操作的 WLAN 安全性增强解决方案，可大大增强现有以及未来无线局域网系统的数据保护和访问控制水平。部署适当的话，WPA 可保证 WLAN 用户的数据受到保护，并且只有授权的网络用户才可以访问 WLAN 网络。

由于 WEP 已证明的不安全性，当时在 802.11i 协议完善前，采用 WPA 为用户提供一个临时性的解决方案。该标准的数据加密采用 TKIP 协议(Temporary Key Integrity Protocol)，认证有两种模式可供选择，一种是使用 802.1x 协议进行认证，另外一种是称为预先共享密钥 PSK(Pre-Shared Key)模式。

预共用密钥模式（pre-shared key，PSK， 又称为个人模式）是设计给负担不起 802.1X 验证服务器的成本和复杂度的家庭和小型公司网络用的，每一个使用者必须输入密语来取用网络，而密语可以是 8 到 63 个 ASCII 字符、或是 64 个 16 进位数字（256 位元）。使用者可以自行斟酌要不要把密语存在电脑里以省去重复键入的麻烦，但密语一定要存在 Wi-Fi 取用点里。

另外一种 802.1x 协议认证模式是通过 802.1X 认证服务器散布不同的钥匙给各个用户，用 802.1X 认证的版本叫做 WPA 企业版或 WPA2 企业版。

WPA 的资料是以一把 128 位元的钥匙和一个 48 位元的初向量 (IV) 的 RC4 stream cipher 来加密。WPA 超越 WEP 的主要改进就是在使用中可以动态改变钥匙的“临时钥匙完整性协定”（Temporal Key Integrity Protocol，TKIP），加上更长的初向量，这可以击败知名的针对 WEP 的金钥匙取攻击。

除了认证跟加密外，WPA 对于所载资料的完整性也提供了巨大的改进。WEP 所使用的 CRC（循环冗余校验）先天就不安全，在不知道 WEP 钥匙的情况下，要篡改所载资料和对应的 CRC 是可能的，而 WPA 使用了称为 “Michael” 的更安全的讯息认证码（在 WPA 中叫做讯息完整性查核，MIC）。进一步地，WPA 使用的 MIC 包含了帧计数器，以避免 WEP 的另一个弱点 - replay attack（回放攻击） - 的利用。

有两个理由使得 WPA 被定位为到达较安全的 802.11 保全之前的过渡步骤：

1. 制定 802.11i 的工作比原先预期的久了很多，在大家越来越担心无线安全性之时竟然花了四年之久；

2. 它包含了与 WEP 相容的 802.11i 子集合，即使是最早的 802.11b 接口卡也能用。

借由增大钥匙和初向量、减少和钥匙相关的封包个数、再加上安全讯息验证系统，WPA 使得侵入无线局域网路变得困难许多。Michael 算法是 WPA 设计者在大多数旧的网络卡也能使用的条件下找到的最强的算法 ,然而它可能会受到伪造封包攻击。为了降低这个风险，WPA 网络每当侦测到一个企图的攻击行为时就会关闭 30 秒钟。

WPA2 是 WPA 的升级版,现在新型的网卡，AP 都支持 WPA2 加密。WPA2 则采用了更为安全的算法。CCMP 取代了 WPA 的 TKIP,AES 取代了 WPA 的 MIC。同样的因为算法本身几乎无懈可击,所以也只能采用暴力破解和字典法来破解。暴力破解是“不可能完成的任务”，字典破解猜密码则像买彩票。可以看到无线网络的环境如今是越来越安全了，同时覆盖范围越来越大，速度越来越快。