WPA 无线网络破解方法与安全防护

文/周瑞华

摘要

网络给我们的生活增添了不少方便与色彩，如今我们的工作、生活基本上已经离不开网络了，大家试想一下如果某一段时间没有了网络你的生活会是怎样的，说到这里不难解析出重要的两点：第一，我们不能没有网络。第二，网络安全保障问题……

【关键词】无线网络 网络安全 安全防护

网络既方便又灵活，很多家庭和企业都配置了无线网络，不少公共场所也可免费无线上网。伴随无线网络应用的增多，无线网络安全问题也日益凸显，无线网络被盗用的情况时有发生，而且最可怕的是无线网络加密也被破解。如何防范这些问题，应成为了大家关注的焦点。

1 主流的WPA/WPA2方式加密认证的无线网络的破解方法

下班后，打开笔记本搜了一下周围的无线网络，无线网络列表中有中国移动的CMCC,0,A, 并且也有好几个信号比较强的私人无线路由器 /AP 信号，我要说大实话：山东潍坊的 CMCC 账号又黑又贵真心不想用！下面介绍用两种方法破解主流的 WPA/WPA2 方式加密认证的无线网络：

1.1 第一种破解WPA密码方法：抓包跑字典法

无线设备在接入到无线网络的时候需要首先进行密码认证，也就是说会把认证密钥发送给认证服务器，这里也就有个不安全因素存在，只要想办法在无线客户端接入网络的时候抓取到其带有安全密钥的数据包，虽说 WPA 里面使用的的 AES 算法是不可逆的！但是我们可以找一堆可能的密码组合(即:密码字典)，将这些可能的密码通过对应的算法加密得到其加密后的密文，然后拿这些密文去跟我们抓取数据包中的认证密文进行对比（跑字典），对比结果如果相同，那么可想而知这个密码就是真正的密码……思路就是这样不多说啦，相信多数有点基础的朋友都能看懂！

下面以实例详细来说一下破解过程：

（1）在 LINUX 系统下打开程序 FeedingBottle 找到需要使用的无线网卡，选中点击【Next->】按钮。

（2）选择对应的加密方式 WPA/WPA2，信道，扫描时间等，然后点击【Scan…】按钮开始扫描周边的无线网络。

（3）注意观察弹出窗口中 Data 项下面的数据，当你想抓包的那个 SSID 的 DATA 项有数据，你就可以手动点击 Stop! 停止啦，因为说明他下面已经有客户端啦，然后在 Aps Information 下面找到对应的 SSID 选中，在 Clients Information 下面就可以看到其客户端的信息，这里如果有多个客户端就选那个数据包多的 - 点击 Next 继续进行【下一步】。

（4）先点击【Start】按钮随便选一个密码字典，这主要是先开启 mon 抓包进程，然后多多点击客户端 MAC 边的 Deauth 按钮进行断开连接攻击，此攻击的作用毋庸置疑就是让客户端与无线路由器断开连接，然后客户端会主动进行重新认证连接，这时候我们就成功抓到带有密码的握手包啦。

（5）这时不建议再继续用里面自带的工具跑密码，因为跑字典太慢啦，还是用 U 盘把 targetap_wpa-01.cap 这个带有密钥的文件弄出来（LINUX 使用 U 盘看下图），最后那条命令是关键，搞完文件之后记得先用 umount 命令卸载设备，然后才能拔出 U 盘。

（6）在 WINDOWS 下做好密码字典，然后就可以用 EWSA 跑字典啦（EWSA 需要设置好）。我跑了一个多小时就跑出了正确的密码——密码是 8 位纯数字的。

1.2 第二种破解WPA密码方法：枚举无线路由器的PIN码

这种方式是我在捉到对应 SSID 的密钥包后，试了各种密码字典 (手机号，8 位以内的数字，弱口令等) 没有枚举出密码的情况下进行的，这种情况说明其设置的无线密码一定比较长或者复杂，有的无线路由器（AP）是支持并开启了 WPS 模式 (WPS 即：WiFi 保护设置)，用心的朋友可能会发现你的无线路由器上面会写着一个 8 位数 PIN 码，这个 PIN 码就是在开启了 WPS 的设备上无线网络客户端可以直接通过此对应 PIN 进行网络接入。一个 8 位数的 PIN 码，一个一个试最多也就试个 99999999 次！这对于计算机来说岂不是小意思……下面还是以实例来大体说一下破解过程吧：

1、首先扫描出对方 SSID 无线路由器（或者 AP）的 MAC 地址（过程略）。

2、在带有 reaver 工具的 LINUX 系统下打开终端用几条命令就能开始 PIN 枚举：

（1）ifconfig wlan0 up：启动 wlan0 网卡。

（2）airmon-ng start wlan0：建立基于 wlan0 无线网卡的监控端口 mon0，开启监视模式。

（3）reaver -I mon0 –b：这里写无线路由器 MAC 地址；-a -S -vv -d 0：这里就是开始枚举破解 PIN 啦 (后面的 -d 0 参数为加快速度，信号不好时可以去掉此参数，破解过程中可以按 CTRL+C 键中断操作，系统会自动保存进度等以后可以接着以前的进度继续破解)。我跑了三晚上，大约 30 个小时才得到的 PIN 码，得到 PIN 码后随即直接给出了 WPA 密码 --12 位数字、字母混合密码。

2 无线网络安全防护的问题

其实关于怎么做才能保障自己的无线网络不被别人蹭网、恶意接入，首先要明白无线网络没有绝对的安全！我下面只能说几点防护措施：

（1）无线连接密码越长越复杂就越难通过直接跑字典的方式获取密码

（2）在没有必要的情况下慎用 WPS 功能，因为你密码再复杂 PIN 码也是 8 位数字，可能通过直接破解 PIN 的方式破解无线网络

（3）如果非要开启无线路由器的 WPS 功能，请定期更改 PIN 码。

（4）必要时可以直接关闭 SSID 广播，SSID 广播的关闭就意味着搜索不到对应路由器的无线网络 SSID，客户端需要连接就只能通过手工输入要连接的 SSID 来进行接入网络。

（5）当然你也可以在路由器里设置只允许绑定的 MAC 进行网络接入。

（6）想做好的安全防护，先学会攻击原理（其实明白人从我上面的破解原理及方式就能总结出来防护措施）。

无线网络是发挥巨大便利性的同时，其安全问题也不容小觑，网络安全重在防护意识，只要大家常关注于此，运用好以上方法，就能大大提高你的网络安全性。

参考文献

[1] 王双剑，丁辉．无线网络安全的机制及相关技术措施 [J]．科技传播 ,2012(03)．
[2] 宋玲．浅议无线网络的安全隐患与防范措施 [J]．科技信息 ,2012(04)．
[3] 田永民．基于无线网络 WLAN 安全机制分析 [J]．数字技术与应用 ,2011(05)．

作者简介

周瑞华（1975 年），女，硕士学位。现为山东省潍坊商业学校讲师。主要研究方向为计算机。

作者单位

山东省潍坊商业学校　山东省潍坊市　261011