

# Wifi 密码破解

- 之 WEP 破解

## 一、引言

相信大家对 wifi 再熟悉不过了,但是当你在享受 wifi 带来的无线上网的方便之时,是否也曾考虑过其安全问题?那 Wifi 的安全性到底如何呢?首相跟大家简要介绍一下,常见的 wifi 加密分为 WEP 加密和 WPA,/WPA2 加密,如图 1,本期主要讨论的是 WEP 加密方式的破解。



## 二、准备工作

Wifi 破解的需要从两个方面来准备。首先硬件方面,你需要有一张支持注入的无线网卡,可以是笔记本内置的无线网卡,也可以是 USB 网卡;其次在软件方面,你需要安装一款 wifi 密码破解软件,如 miniwep (本期会用 minidwep 来为大家演示)。

### 三、破解 WIFI 密码

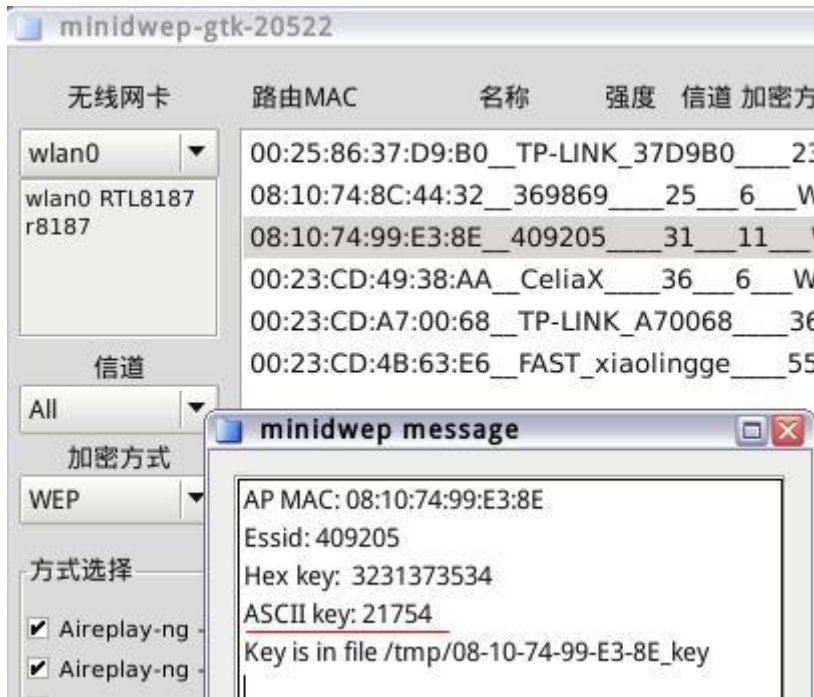
在启动了 miniwep 之后，点击扫描，会显示当前能接收到信号的所有 AP



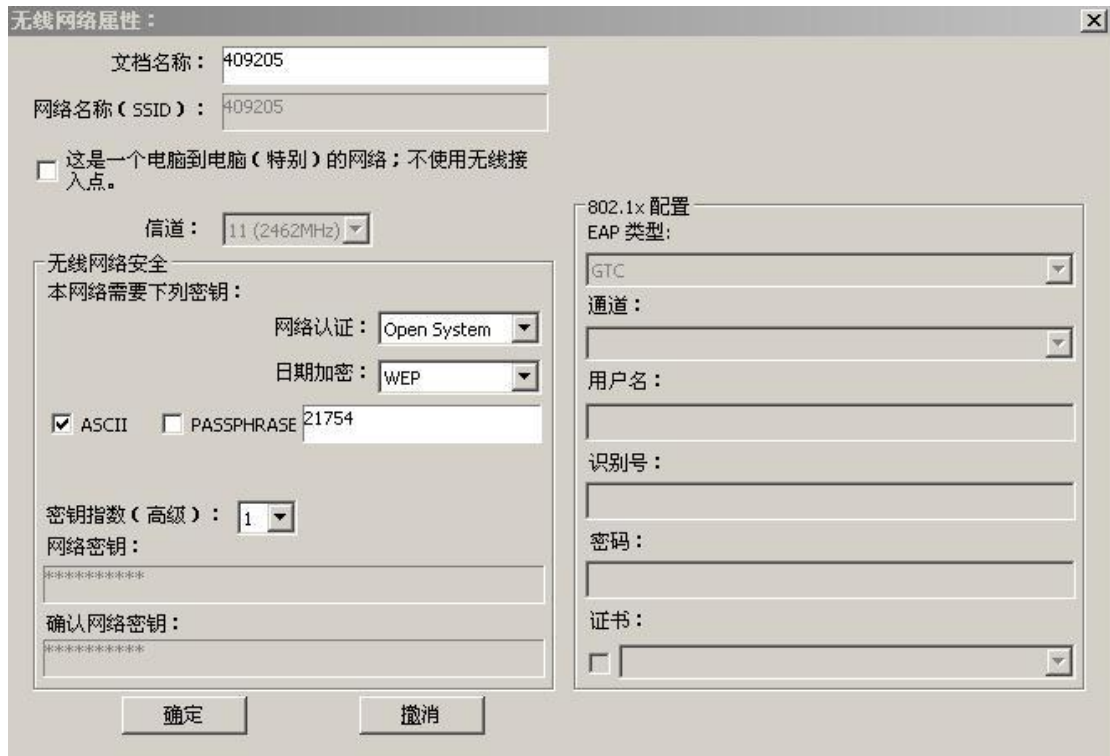
然后选中你想要破解的 AP，点击启动，你会发现下角的 IVS 数量在急速增多



等到 IVS 数量增加到一定时（一般是 20000 左右），Wifi 密码就破解完成了，图中的 ASCII key 后面的就是 wifi 密码



如果是 USB 网卡的用户，还需要对 wifi 进行设置后才能使用



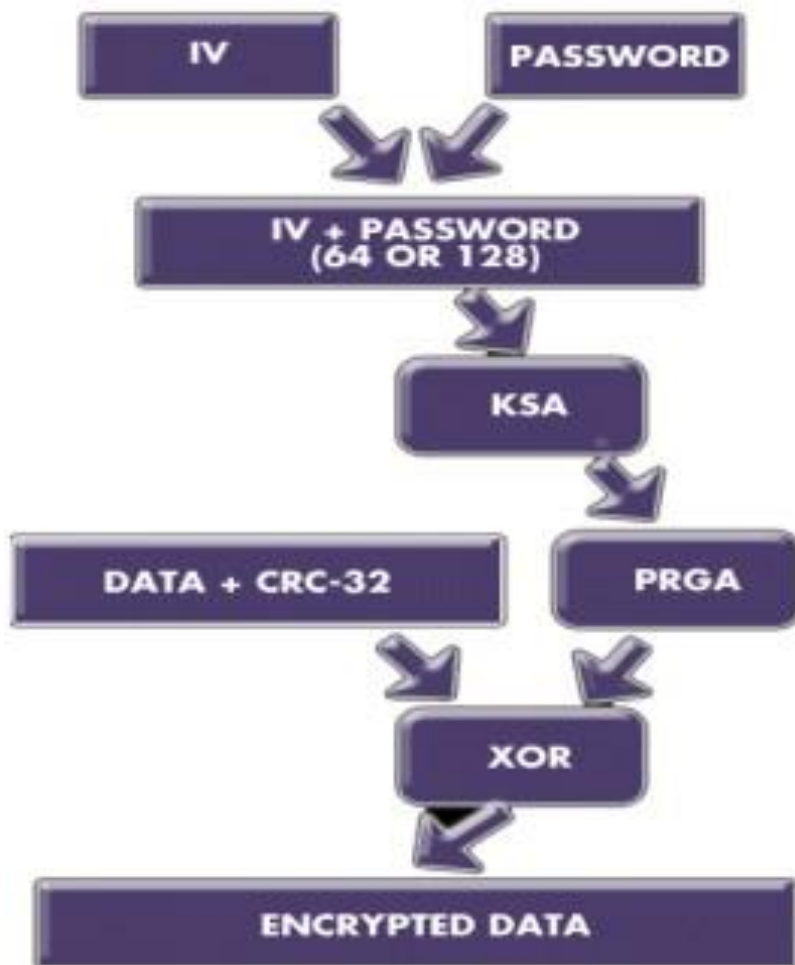
配置完成之后就能使用该 wifi 了，如图 6



## 四、原理

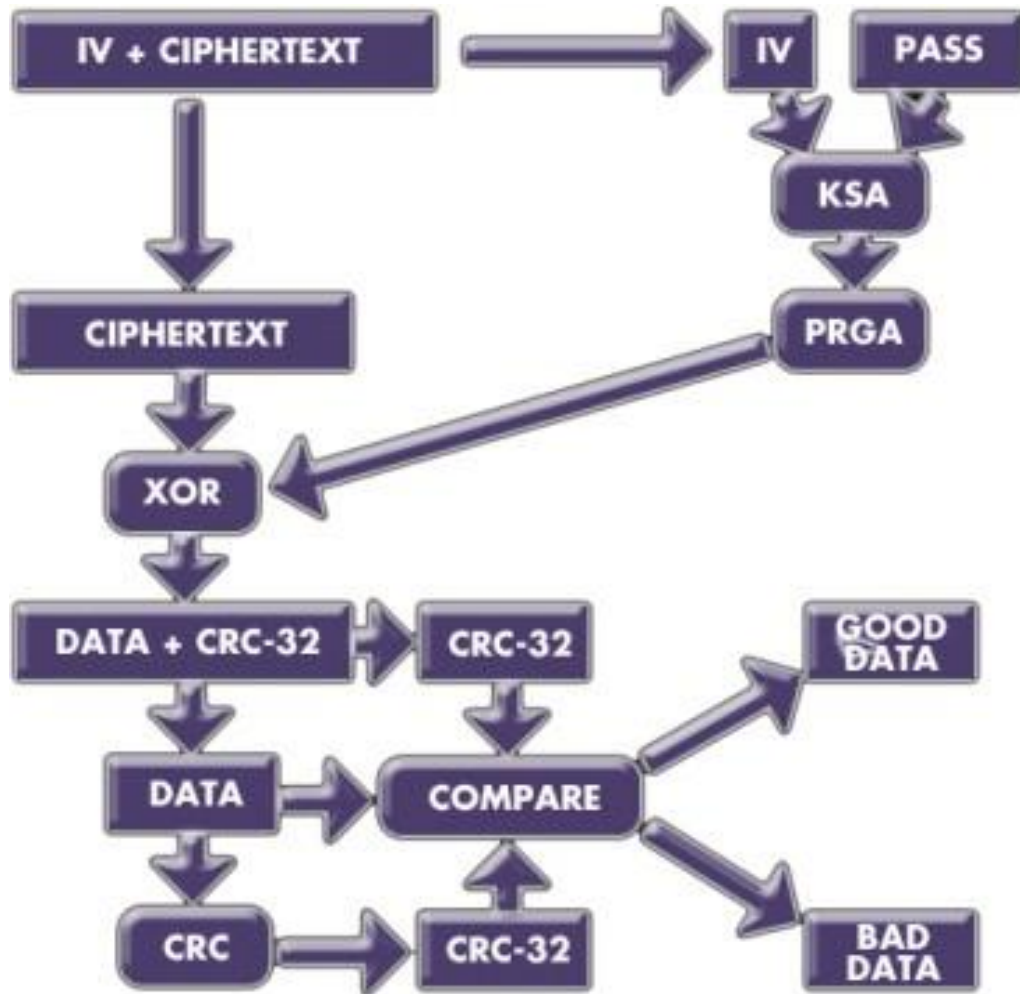
看完了刚才破解 WEP 加密的过程，大家是否心生疑问，问什么 WEP 加密会如此脆弱呢？那么这还要从 WEP 加密方式说起。

WEP (Wired EquIValent PrIVacy) 叫做有限等效加密，是一种可选的链路层安全机制，用来提供访问控制，数据加密和安全性检验等。WEP 的加密过程如下图所示。



其中 IV 为初始化向量，PASSWORD 为密码  $KSA=IV+PASSWORD$ 。DATA 为明文 CRC-32 为明文的完整性校验值  $PRGA=RC4(KSA)$  的伪随机数密钥流 XOR 异或的加密算法。ENCRYPTED DATA 为最后的密文。最后 IV+ENCRYPTED DATA 一起发送出去。

同时，在接收端会解密，如下图所示



CIPHERTEXT 为密文。它采用与加密相同的办法产生解密密钥序列，再将密文与之 XOR 得到明文，将明文按照 CRC32 算法计算得到完整性校验值 CRC-32'，如果加密密钥与解密密钥相同，且 CRC-32' = CRC-32，则接收端就得到了原始明文数据，否则解密失败。

WEP 加密方式在设计之初试图以其加密算法保证通信的安全性，以对抗窃听，以 CRC32 算法作为完整性检验，以对抗对数据的篡改。但是 WEP 真的安全吗？不幸的是 CRC32 算法作为数据完整性检验算法，由于其本身的特点非但未使 WEP 安全性得到加强，反而进一步恶化。首先 CRC 检验和是有效数据的线性函数，这里所说的线性主要针对异或操作而言的，即  $C(x \oplus y) = C(x) \oplus C(y)$ 。利用这个性质，恶意的攻击者可篡改原文 P 的内容。特别地，如果攻击者知道要传送的数据，会更加有恃无恐。其次，CRC-32 检验和不是加密函数，只负责检查原文是否完整，并不对其进行加密。若攻击者知道 P，就可算出  $RC4(v, k)$  ( $RC4(v, k) = P \oplus (P \oplus RC4(v, k))$ )，然后可构造自己的加密数据  $C' = (P', C(P')) \oplus RC4(v, k)$  和原来的 IV 一起发送给接收者(802.11b 允许 IV 重复使用)。

根据上面的信息，我们可以知道 WEP 是存在缺陷的，那么 WEP 加密具体是如何被破解的呢？

1. 监听模式被动破解(这个就是有客户端并有大量有效通信)。

我们知道要还原出 WEP 的密码关键是要收集足够的有效数据帧，从这个数据帧里我们可以提取 IV 值和密文。与对于这个密文对应的明文的第一个字节是确定的他是逻辑链路控制的 802.2 头信息。通过这一个字节的明文，还有密文我们做 XOR 运算能得到一个字节的 WEP 密钥流，由于 rc4 流密码产生算法只是把原来的密码给打乱的次序。所以我们获得的这一次字节的密码就是就 IV+PASSWORD 的一部分。但是由于 RC4 的打乱。不知道这一个字节具体的位置很排列次序。当我们收集到足够多的 IV 值还有碎片密码时，就可以进行统计分析运算了。用上面的密码碎片重新排序配合 IV 使用 RC4 算法得出的值和多个流密码位置进行比较。最后得到这些密码碎片正确的排列次序。这样 WEP 的密码就被分析出来了。

2. 主动攻击(有客户端。少量通信或者没有通讯)

-3 ARP-request attack mode 攻击抓取合法客户端的 arp 请求包。如果发现合法客户端发给 AP 的 arp 请求包，攻击者就会向 AP 重放这个包。由于 802.11b 允许 IV 重复使用。所以 AP 接到这样的 arp 请求后就会回复客户端。这样攻击者就能搜集到更多的 IV 了。当捕捉到足够多的 IV 就可以按上面的 2.9.1 里的进行破解了。如果没有办法获取 arp 请求包我们就可以用 -0 攻击使得合法客户端和 AP 断线后重新连接。-0 Deauthenticate 攻击实际就是无线欺骗。这样我们就有机会获得 arp 请求包了。

3. 主动攻击(没有客户端的模式)

先和 AP 进行伪链接-1 fakeauth count attack mode。这样就能产生数据包了。收集两个 IV 相同的的 WEP 包，把这两个包里的密文做 XOR 运算。得到一个 XOR 文件。用这个 XOR 文件配合伪造 arp 包的工具。利用 CRC-32 的特点伪造一个 arp 包和原来的 IV 一起发给 AP。这样就可以按上面 2.9.2 里的进行破解了。其中 -2 Interactive, -4 Chopchop, -5 Fragment 都是属于上面这个攻击类型的。

通过本期的介绍，相信大家对 WEP 加密方式的 wifi 有了进一步的了解，那么想知道 WPA 加密方式的 wifi 是什么情况吗？敬请关注下一期 Wifi 密码破解之 WPA 破解。