中国无线论坛

http://www.wlanbbs.com/

论坛 ID 0o90o9 QQ3040165

深入 WEP 和 WPA 密码原理

1 概述

目前情况下：

WEP 的破解为利用加密体制缺陷，通过收集足够的数据包，使用分析密算法还原出密码。

WPA 目前没有加密体制的缺陷可被利用，破解 WPA 密码使用的是常规的字典攻击法。

所以在破解方式上 WEP 和 WPA 有很大差异。

2 WEP

2.1 （Wired EquIValent PrIVacy，WEP）

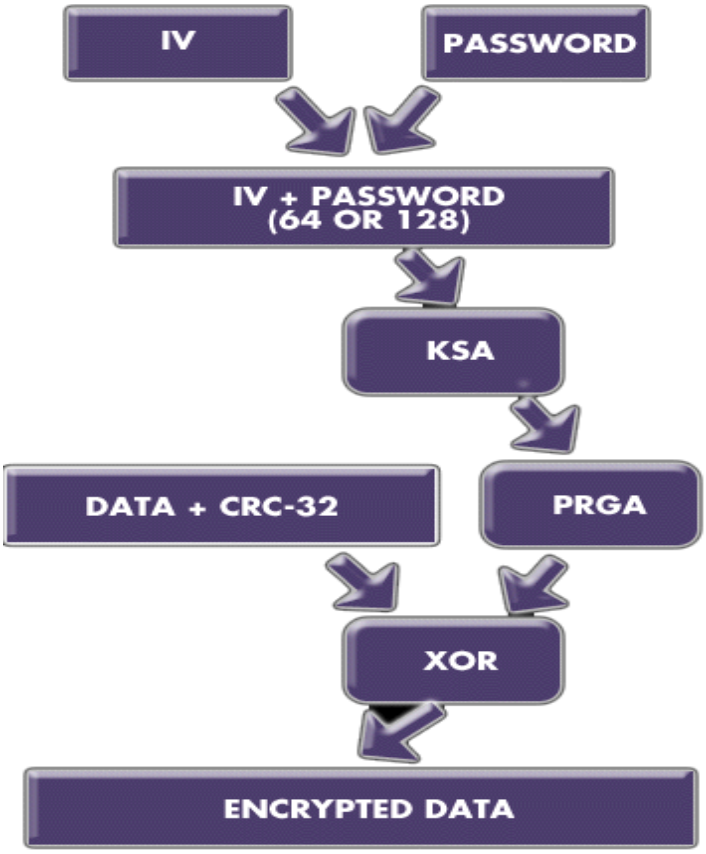
叫做有线等效加密。掌握 WEP 破解的人，肯能会说 WEP 不如有线的安全性高。但这发生在 WEP 的很多弱点被发现之后。也是由于 WEP 的弱点导致 WPA 的出现。

2.2 （WEP）算法

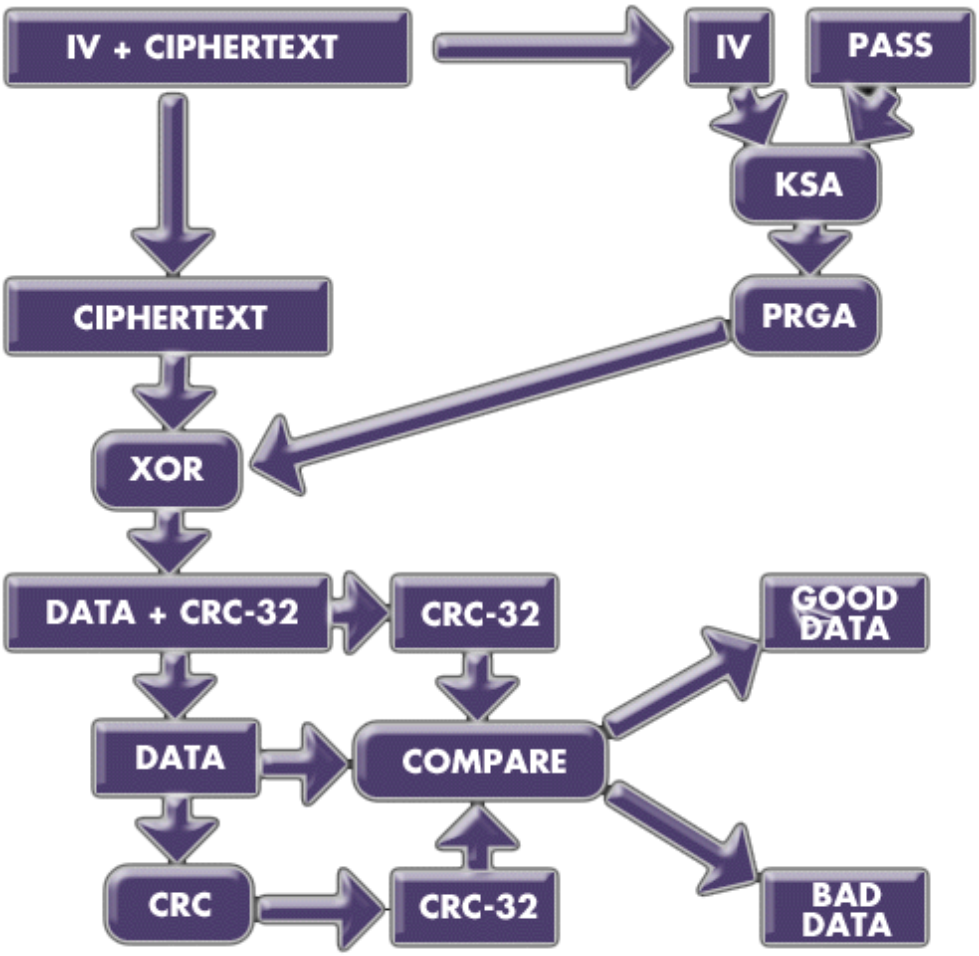
WEP 算法是一种可选的链路层安全机制，用来提供访问控制，数据加密和安全性检验等。802.11 定义了 WEP 算法对数据进行加密。

2.3 加密过程如图所示。

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。



2.4　接收端的解密过程如图所示。



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。

2.5 WEP 算法通过以上的操作试图达到以下的目的

采用 WEP 加密算法保证通信的安全性，以对抗窃听。

采用 CRC32 算法作为完整性检验，以对抗对数据的篡改。

2.6 WEP 算法之死

95 9 月 RC4 潜在的威胁性(wanger)

00 10 月 通过分析 wpe 包获取密码(walker)

01 5 月 针对于明文攻击的一个推论(Arbaugh)

01 7 月 针对于 CRC32 的攻击(Borisov， Goldberg，Wagner)

01 8 月 针对于 RC4 的攻击(S。Fluhrer， I。Martin 和 A。Shamir)

01 8 月 airosnort 发布

02 2 月 改进的攻击算法(h1kari)

04 8 月 chopchop 攻击出现

04 7/8 月 aircrack 出现(Devine，Sanchez)

2.7 WEP 的破解理论是在 01 年 8 月就变得可行了

S.Fluhrer， I.Martin 和 A.Shamir 合作研究发现了对无线局域网安全性最致命的攻击。利用 WEP 帧的数据负载中部分已知信息来计算出该 WEP 帧所使用的 WEP 密钥。由于 WEP 加密算法实际上是利用 RC4 流密码算法作为伪随机数产生器，将由初始矢量 IV 和 WEP 密钥组合而成的种子生成 WEP 密钥流，再由该密钥流与 WEP 帧数据负载进行异或运算来完成加密运算。而 RC4 流密码算法是将输入种子密钥进行某种置换和组合运算来生成 WEP 密钥流的。由于 WEP 帧中数据负载的第一个字节是逻辑链路控制的 802.2 头信息，这个头信息对于每个 WEP 帧都是相同的，攻击者很容易猜测，利用猜的第一个明文字节和 WEP 帧数据负载密文就可以通过异或运算得到 PRNG 生成的密钥流中的第一字节。另外，种子密钥中的 24 比特初始矢量是以明文形式传送的，攻击者可以将其截获，存到初始矢。S.Fluhrer， I.Martin 和 A.Shamir 证明：利用已知的初始矢量 IV 和第一个字节密钥流输出，并结合 RC4 密钥方案的特点，攻击者通过计算就可以确定 WEP 密钥。

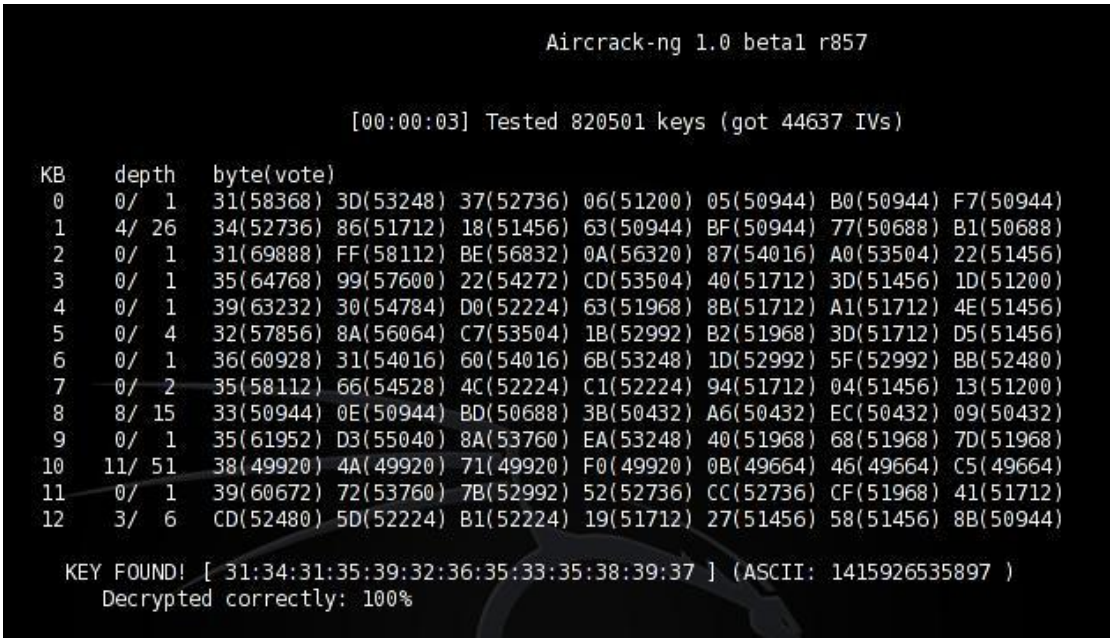
2.8 CRC－32 算法缺陷

CRC－32 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⊕(P⊕RC4(v，k))，然后可构造自己的加密数据 C'=(P'，C(P')) ⊕ 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)。

2.9 WEP 密码如何被破解出来的

2.9.1 监听模式被动破解(这个就是有客户端并有大量有效通信)

根据已知的的信息。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。下图就是 WEP 破解过程。有助于你理解破解 WEP 通过分析子密码还原密码的过程。



2.9.2 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 Deautenticate 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。

2.9.3 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。

2.10 WEP 的安全弱点

A.802.2 头信息和简单的 rc4 流密码算法

导致攻击者在有客户端并有大量有效通信时，可以分析出 WEP 的密码。

B.IV 重复使用

导致在攻击者在有客户端。少量通信或者没有通讯时，可以使用 arp 重放的方法获得大量有效数据。

C．无身份验证机制，使用线性函数 CRC32 进行完整性校验。

无身份验证机制，导致攻击者能使用-1 fakeauth count attack mode 和 AP 建立伪链接。进而获得 XOR 文件。使用线性函数 CRC32 进行完整性校验，导致攻击者能用 XOR 文件伪造一个 arp 包。然后依靠这个包去捕获大量有效数据。

2.11 WEP 窃听

由于 WEP 全局都是用 IV+WEP 密码来保护明文的。当有了密码后攻击者可以使用同样的算法能随时任意窃听任意 STATION 至 AP 之间的通讯。这样的窃听对于网银这样的双向认证的安全不会有影响。但是在 ip 包里的明文用户名和密码就很容易被窃听到了。例如登录 AP 的用户名和密码。由于无线网络窃听的存在，在使用交换机的有线网络中用关闭 dhcp 设置陌生网段的来禁止非法访问的方式。不在适合于无线网络。攻击者完全能根据窃听到的合法客户端数据包配合已知密码来分析出 ip 的真实配置。

2.12 WEP 的现状

WEP 真的不是一种强壮的加密方式对于那种不怀好意的攻击者。无法胜任在安全有求比较高的场所。对于安全较低的厂所只能说有胜于无。

3 WPA

3.1 WPA 加密算法的的两个版本介绍

WPA = 802.1x + EAP + TKIP + MIC
= Pre-shared Key + TKIP + MIC

802.11i(WPA2)
= 802.1x + EAP + AES + CCMP
= Pre-shared Key + AES + CCMP

这里 802.1x + EAP，Pre-shared Key 是身份校验算法 （WEP 没有设置有身份验证机制）
TKIP 和 AES 是数据传输加密算法 （类似于 WEP 加密的 RC4 算法）
MIC 和 CCMP 数据完整性编码校验算法 （类似于 WEP 中 CRC32 算法）

3.2 WPA 认证方式

802.1x + EAP （工业级的，安全要求高的地方用。需要认证服务器）
Pre-shared Key （家庭用的，用在安全要求低的地方。不需要服务器）

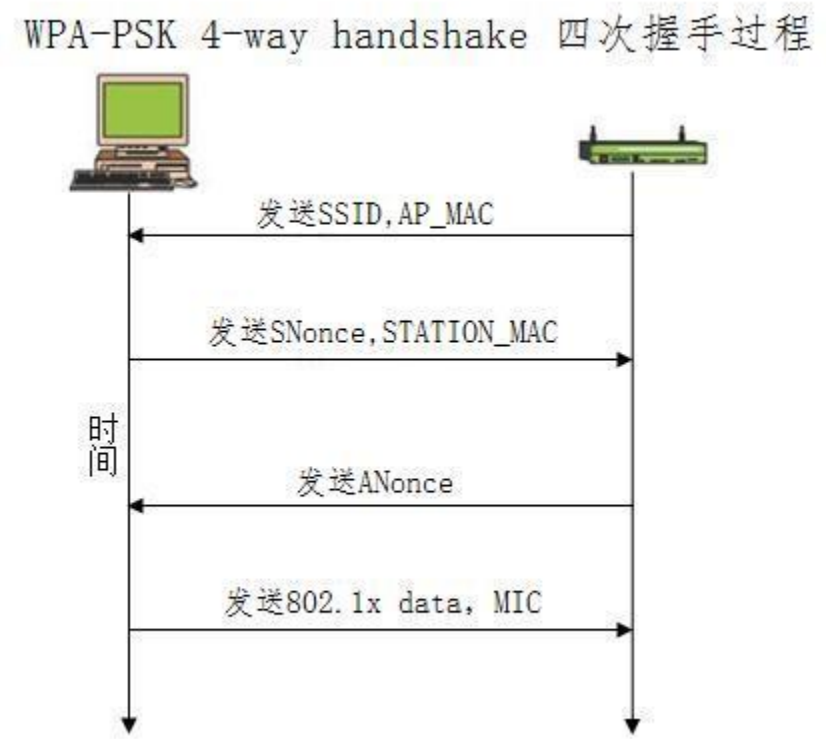
EAP 扩展认真协议，是一种架构。而不是定义了算法。常见的有 LEAP，MD5，TTLS，TLS，PEAP，SRP，SIM，AKA 其中的 TLS 和 TTLS 是双向认证模式。这个和网络银行的安全方式差不多。这个认证方式是不怕网络劫持和字典攻击的。而 md5 是单向认证的。不抗网络劫持，中间人攻击。关于企业级的如何破解就不讨论了。因为论坛上也很少提到。本身 EAP 模式是个协议，不是算法。

3.3 WPA-PSK

论坛上破解 WPA 也主要是集中在这个模式上的。我们都知道破解 WPA-PSK 不是和 WEP 一样抓很多包就能破解的。关键是要获取握手包，这个握手包叫 4way-handshake 四次握手包。那么我们就从这个四次握手包开始。

3.4 四次握手

通信过程如图



3.4.1 WPA-PSK 初始化工作

使用 SSID 和 passphares 使用以下算法产生 PSK 在 WPA-PSK 中 PMK=PSK

PSK=PMK=pdkdf2_SHA1(passphrase，SSID，SSID length，4096)

3.4.2 第一次握手

AP 广播 SSID，AP_MAC(AA)→STATION

STATION 端

使用接受到的 SSID，AP_MAC(AA)和 passphares 使用同样算法产生 PSK

3.4.3 第二次握手

STATION 发送一个随机数 SNonce，STATION_MAC(SA)→AP

AP 端

接受到 SNonce，STATION_MAC(SA)后产生一个随机数 ANonce

然后用 PMK，AP_MAC(AA)，STATION_MAC(SA)，SNonce，ANonce 用以下算法产生 PTK

PTK=SHA1_PRF(PMK， Len(PMK)， "Pairwise key expansion"，MIN(AA，SA) || Max(AA，SA) || Min(ANonce，SNonce) || Max(ANonce，SNonce))

提取这个 PTK 前 16 个字节组成一个 MIC KEY

3.4.4 第三次握手

AP 发送上面产生的 ANonce→STATION

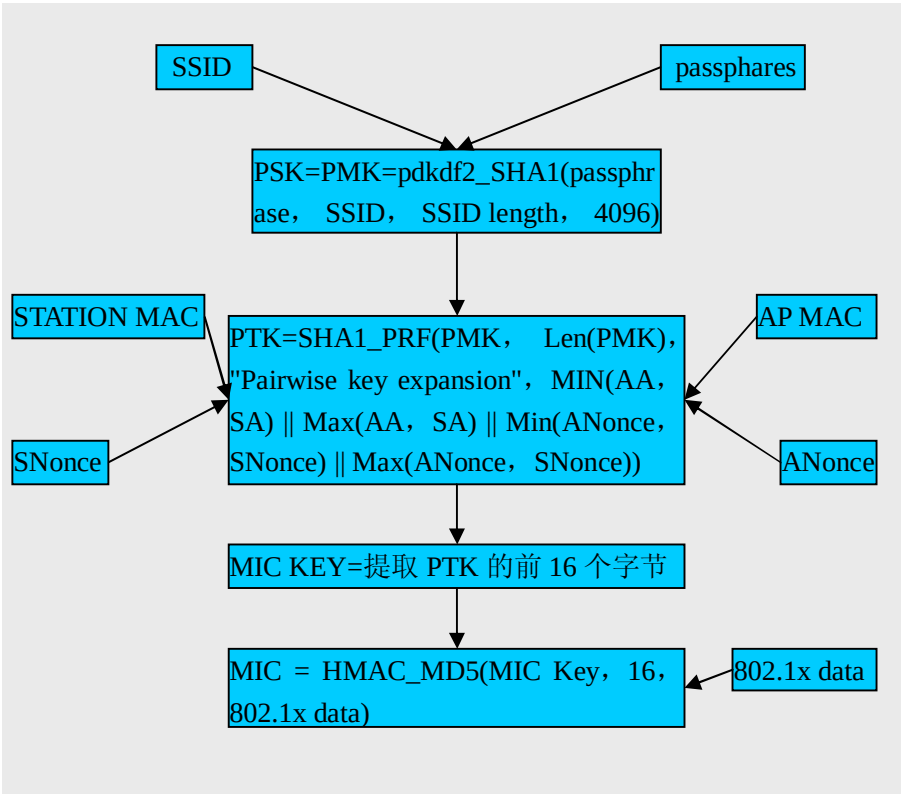
STATION 端

用接收到 ANonce 和以前产生 PMK，SNonce，AP_MAC(AA)，STATION_MAC(SA)用同样的算法产生 PTK。
提取这个 PTK 前 16 个字节组成一个 MIC KEY
使用以下算法产生 MIC 值
用这个 MIC KEY 和一个 802.1x data 数据帧使用以下算法得到 MIC 值
MIC = HMAC_MD5(MIC Key，16，802.1x data)

3.4.5 第四次握手

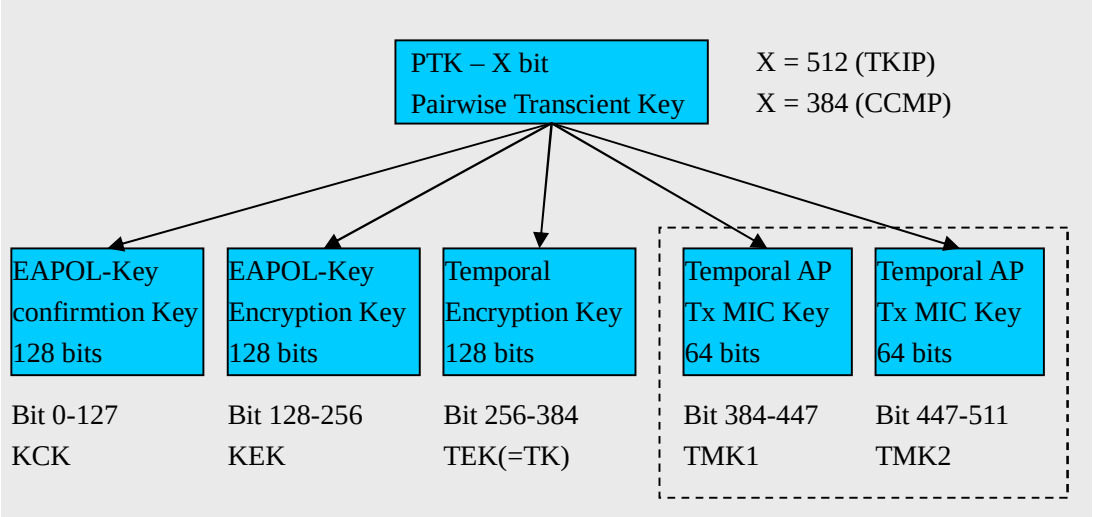
STATION 发送 802.1x data ，MIC→AP
STATION 端
用上面那个准备好的 802.1x 数据帧在最后填充上 MIC 值和两个字节的 0（十六进制）让后发送这个数据帧到 AP。
AP 端
收到这个数据帧后提取这个 MIC。并把这个数据帧的 MIC 部分都填上 0（十六进制）这时用这个 802.1x data 数据帧，和用上面 AP 产生的 MIC KEY 使用同样的算法得出 MIC’。如果 MIC’等于 STATION 发送过来的 MIC。那么第四次握手成功。若不等说明则 AP 和 STATION 的密钥不相同，或 STATION 发过来的数据帧受到过中间人攻击，原数据被篡改过。握手失败了。

3.4.6 MIC 的派生图



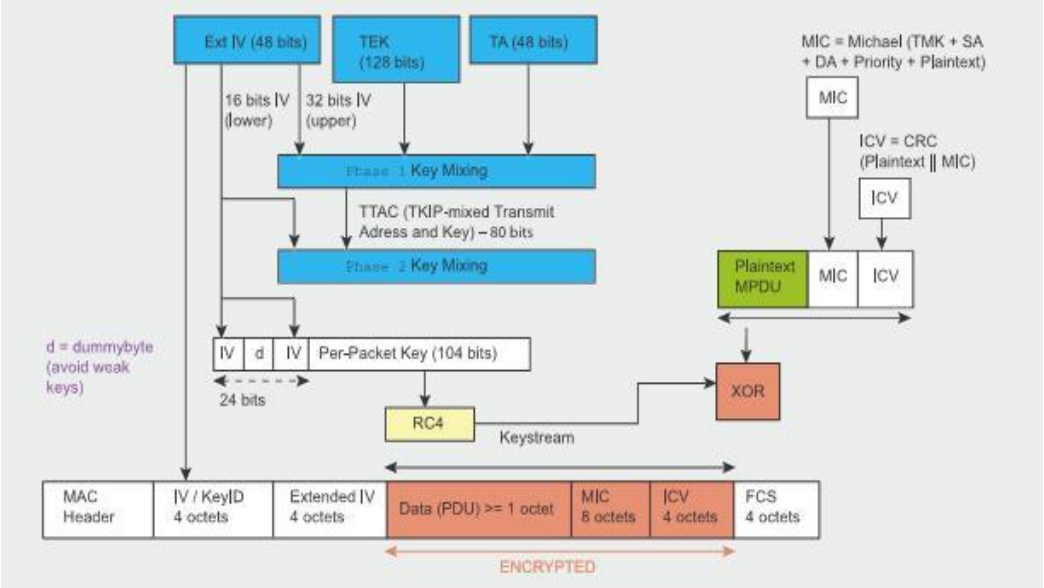
3.5 AP 和 STATION 之间的加密通信

3.5.1 通讯使用的临时 KEY 的派生图

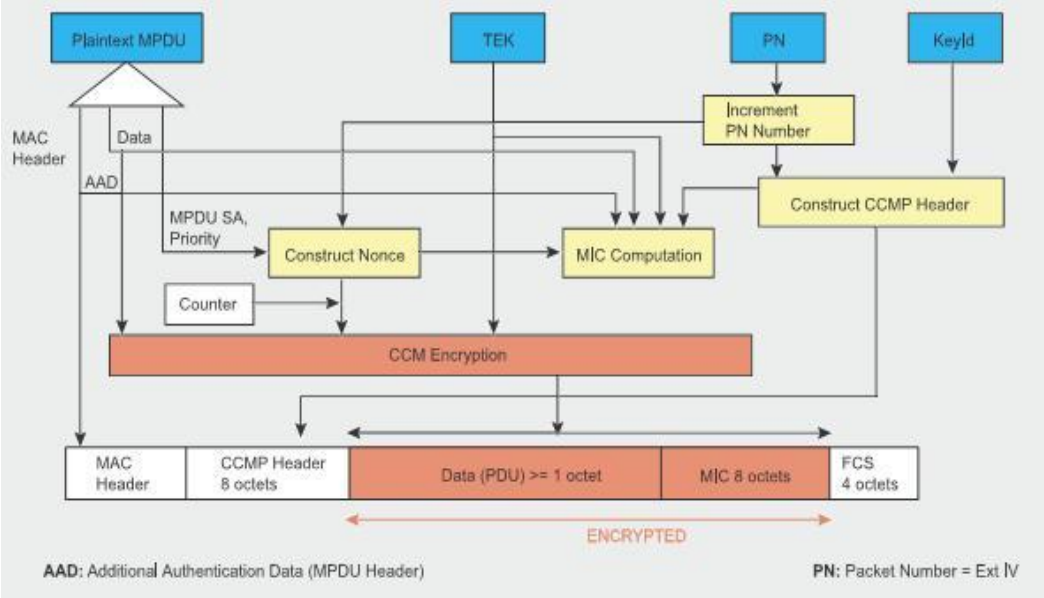


3.5.2 使用 KEY 进行加密通信

3.5.2.1 TKIP



3.5.2.2 CCMP



3.5.3 WPA 安全规则

针对于 WEP 的安全漏洞 WPA 也相应更新了安全规则：

A． 增强至 48bit 的 IV。

B． Sequence Counter，防止 IV 重复。

C． Dynamic key management，动态 key 管理机制。

D． Per-Packet Key 加密机制，每个包都使用不同的 key 加密。

E． MIC (Message Integrity Code)<Michael>，信息编码完整性机制。

解说：动态 key 管理机制

在通讯期间：

如果侦测到 MIC 错误，将会执行如下程序。

记录并登录 MIC 错误，60 秒内发生两次 MIC 错误。

反制措施会立即停止所有的 TKIP 通讯。

然后更新数据加密的用的 TEK。

3.5.4 WPA 安全机制作用

a. 加密通信流程图、Per-Packet Key 加密机制、动态 key 管理机制使得使用类似于 WEP 中分析子密码攻击的方案，在 WPA 中将变得异常困难，和不可实现。
b. 身份验证机制杜绝了-1 fakeauth count attack mode，建立伪连的攻击。
c. 增强至 48bit 的 IV、防止 IV 重复、MIC 信息编码完整性机制。使得要伪造一个合法数据包变得异常的困难。同时也致使-2 Interactive，-4 Chopchop，5 Fragment 此类攻击对于 WPA 无效。

解说：

a. 虽然 TKIP 使用的是和 WEP 一样的加密算法 RC4，但是 TKIP 中使用 Per-Packet Key 加密机制配合 RC4。这样弥补了 RC4 加密算法的不足。抵抗基于 RC4 漏洞的攻击。WPA2 中的 AES 比 TKIP 有更高的安全性，对他的破解难度就更高了。
b. 使用非线性的 MIC 信息编码完整性算法，取代线性的 CRC-32。增加了攻击者伪造合法数据的难度。

有以上结论我们不难得出一个事实。类似于 WEP 中的无客户端破解密码的做法在 WPA 中是不存在的。

3.6 针对 WPA 的破解攻击

3.6.1 抓取数据传输包进行破解

上面已经明确的指出无论数据传输算法是 TKIP 还是 AES。使用类似于 WEP 中捕获数据包进行分析破解的方式对于 WPA 几乎是不可能的。

3.6.2 抓取 WPA-PSK 的四次握手包进行破解

可以说 WPA-PSK 安全体系是十分完善的。但他始终是用一个密码保护的。对于这种用密码保护的安全体系。一般情况下我们都可以用一种叫字典攻击的常规攻击手段。所以针对 WPA-PSK 可以进行的直接攻击，目前就只有字典攻击这一种方式。而这种常规的攻击方式将在字典攻击里详细讨论。当然我们 WPA-PSK 的设计者也很明确这点，所以在 WPA-PSK 的安全体系中加入了潜规则加以对抗。这点将在攻击预算里做详细的讨论。在 WPA-PSK 的四次握手包中包含着和密码有联系的信息，依靠这个信息进行字典攻击。

3.6.3 断线攻击

由于 WPA-PSK 是单向认证的。所以可以使用 -0 Deautenticate 攻击。这样有助于我们获取握手包。在获得握手包时-0 攻击不要太多，否则适得其反的。有些 AP 几次握手不成就会认为有攻击。禁止客户端和 AP 的链接 30 秒。（可能基于 WPA EAP TLS 这样双向认证的就不怕断线攻击了）

3.6.4 间接攻击

例子：别人输密码你在哪里偷看。使用美人计骗取密码。有技术含量点的。原来 WEP 时他的计算机有漏洞你给他下了木马。改成 WPA 后木马把密码发给你的。或你整天窃听他的 WEP 通信，他改密 WPA 模式时发给路由的密码让你截获了。比较狠一点的，AP 是你卖给他的 AP 的系统里添加了你的后门。

3.7 WPA 安全性的前景

WEP 由原来的安全到今天的不安全。你是否同样也会担心是不是很多年之后的 WPA 也会是同样的命运。但我们也要看到 WEP 的破解不是某个算法的漏洞导致的。而是整个 WEP 的安全体系有很多漏洞所共同导致的。而 WPA 的安全体系很强壮。使用的大多是混合算法。所以某一个算法的弱点往往不能给 WPA 这样的安全体系以致命的打击。WPA 这种依靠算法的安全体系也许某一天会被破解。但是可能 WPA 被完全破解的那一天比 WPA 废弃的那一天都晚。如果这样的话，那么的确该说 WPA 是一种很强壮的安全体系。

3.8 WPA 的窃听

WP-PSK 没有密码几乎没法窃听他的通信。在有了密码的情况下 WPA 的窃听也不具有 WEP 中窃听的随意性。在 WPA 中 SNonce，ANonce 也很好的起到了加密数据防止窃听的作用，所以作为攻击者我们必须从握手开始窃听。而且会同步更替数据加密密钥。所以 WPA-PSK 的安全性都依赖于密码。

3.9 WPA 评价

无论是 WPA 还是 WPA2 在目前都是有很好的安全性的。企业级 EAP 的安全模式更为 WPA 的安全性如虎添翼。我很欣赏 WPA = PSK + TKIP + MIC 这个模式。因为原来 WEP 的设备只需要更换代码就能升级到这个模式了。所以这个模式使用较低的成本就可以实现很高的安全性，还有便捷性。成本当然也是一个东西是否能普及重要因素。而 WPA2　AES+CCMP 的更高的安全性对硬件的要求也是要高一点的。

4　字典攻击

4.1　寻找可以攻击的信息元素

字典攻击作为一种常用的攻击手段要明白的是从那里开始攻击。要寻找和密码有有联系的信息元素。在 WPA 中和密码有联系的信息有数据的传送包和四次握手包。由于无法知道明文，和 WPA 的数据加密算法的复杂性。在数据传输包上要找到可以攻击的信息元素基本上很难实现。所以只能在握手包里寻找有密码有联系的信息。在上面的四次握手包的图片中很清楚的表明，在四川握手中主要传递的有如下数据：SSID，AP_MAC，STATION_MAC，SNonce，ANonce，802.1x data，MIC。前面 6 个元素很清楚，一般不会和密码有联系的。只有最后一个 MIC 和密码有所联系。通过 MIC 的派生图我们知道，MIC 是通过上面六个信息元素和密码通过三个主要的算法派生出来的。那么我们是不是只要找到这三个算法的逆反算法就可以根据上面的 7 个信息元素把密码计算出来了呢。的确实这样。但是这三个算法有一个共同的名字叫 HASH 函数。

4.1.1　HASH 函数

HASH 函数是不可能从生产的散列值来唯一的确定输入值。

a. 单向性(one-way)。HASH 函数是没有反函数的。
b. 抗冲突性(collision-resistant)。要寻找两个 hash 值相同的原值十分困难。
c. 映射分布均匀性和差分分布均匀性。不像普通函数那样数值分布有一定规律。

由于上面的 pdkdf2_SHA1,SHA1_PRF,HMAC_MD5 是 HASH 函数。所以我们就基本上无法直接计算出密码。对于 HASH 函数比较有效的攻击就是建立 HASH 字典攻击。HASH 字典就是把预先算好的 HASH 值按照线性排列然后组成一个数据库。当我们知道一个 HASH 值时在这个数据库里能马上找到他的原值。当然这个过程是通过数据库实现的而不是 HASH 的逆反函数。所以有些 HASH 值在这样的数据库里是找不到原值的。由于 HASH 库是线性的所以。所以在 HASH 库里找数据是十分迅速的。下面的链接让你体验一下 HASH 线性库的速度 http://www.cmd5.com/。还有一点有的人也知道的国内的王小云教授对于部分 HASH 算法有突出贡献的。她的主要贡献是寻找碰撞值。暴力破解的话就是大概需要 2^80 量级的 MD5 HASH 运算。被王教授提高到只需要 2^69 量级的 MD5 HASH 运算就能够找到一个碰撞。我们有这样两个对付 HASH 函数的方法。那么对我们破解我怕密码是不是如虎添翼了呢？

4.1.2　HMAC (HASH Message Authentication Code)哈希消息校验算法

这里我承认我刚才有骗过你。pdkdf2_SHA1,SHA1_PRF,HMAC_MD5 不是 HASH 函数。当然我骗你我也有我的理由啦。第一我以前被别人骗过，某论坛上说建立 HASH 库然后进行 WPA 破解的。能建立 HASH 库那三个函数不是 HASH 函数那是什么啊。第二我不是故意的。了解 HASH 函数，有助于你理解 HMAC 算法。所以 pdkdf2_SHA1,SHA1_PRF,HMAC_MD5 是 HMAC 算法。不是 HASH 函数。HMAC 算法

就是用一个密码，和一个消息。最后生成一个 HASH 值。由上面的介绍，我们可以看出，HMAC 算法更象是一种加密算法，它引入了密钥，其安全性已经不完全依赖于所使用的 HASH 算法。 所以上面对 HASH 的攻击，对于 HMAC 是没有效果的。HMAC 特别是象“挑战/响应”身份认证应用中，由于攻击者无法事先获得 HMAC 的计算结果，对系统的攻击只能使用穷举或“生日攻击”的方法，但计算量巨大，基本不可行。所以，在目前的计算能力下，可以认为 HMAC 算法在“挑战/响应”身份认证应用中是安全的。

4.1.3 四次握手包

有上面的 HMAC 的特性我们也不难得出 SSID，AP_MAC，STATION_MAC，SNonce，ANonce，802.1x data，这些信息元素都是上面的 HMAC 算法里的消息。HMAC 算法里的密码在 pdkdf2_SHA1 算法里是 WPA 的密码，在 SHA1_PRF 算法里是 PMK，在 HMAC_MD5 算法里是 PTK。最后才得出 MIC 值。由于这些消息和这个 MIC 值都有关联性。所以四次握手吧的后面三次是缺一不可的。而且是有时效性的。不能把不是同一次的握手包拼起来使用的。当然第一次握手包的 SSID 和 AP-MAC 是可以后获取的。这里你也明白了四次握手中根本是不是在传递一个简单的 HASH 值。而是要传递一个 HMAC 值。如果是传递一个简单的 HASH 值，那么我们只要获取后重播这个值就可以欺骗 AP 获得认证了。都不要知道这个 HASH 值对应的原值。但我的这么好的想法被 HMAC 给打破了。

4.1.4 面向于四次握手包的字典攻击。

字典攻击，就是把密码的可能性罗列起来组成一个密码字典。然后把字典里的密码和 SSID，AP_MAC，STATION_MAC，SNonce，ANonce，802.1x data，这些信息元素。通过 pdkdf2_SHA1,SHA1_PRF,HMAC_MD5 这些算法最后生成 MIC’（具体过程看上面 MIC 派生图）。当在字典里找到一个密码他的 MIC’等于握手包中的 MIC。这时字典破解成功。这就是我们要的那个密码。如果把字典里的所有密码都找遍了还有没有符合上述条件的。那么破解失败。

4.2 WPA-PSK 密码规范和可能的密码空间

4.2.1 HEX 模式

64 个的十六进制数字。

4.2.2 ASCII 模式

密码至少 8 位最大不能超过 63 位。字符要求 a～z，A～Z，任意字符包括空格。所以一共可是使用的字符个数为 95 个。

这两种模式的密码的穷举字典（罗列所有的可能性）是超乎想象的大（不包括那想象特别大的人）。我们就拿 HEX 模式的穷举打个比方吧。如果用一个水分子比作是一个密码的话。那么穷举字典里的密码组成一个圆球。这个球的直径是 2.4 光年。而 ASCII 模式密码空间，你别逗了！我们可能观察到的最广阔宇宙空间的直径只可能在 150 亿光年这样的范围之内。这样水球都还需要在那个基础上在大上百万倍。密码空间有时会形成超天文数字的。当然我们不需要尝试像上面一样如此多的数值。因为 MIC 值只有 128 位，我们只需要上面的球和月亮这么大的尝试就能找到一个符合的 MIC。但是这个找到的值可能可以成功握手。但不一定能正常通讯。这样的值可能就是一个 MIC 的碰撞值。他的 MIC 是相同的但是 PMK 是不同的。所以需要尝试所有 PMK 的可能性，而 256 位 PMK 的穷举组成的水球直径还是 2.4 光年。根据 WPA 的密码规范，使用字典攻击法，如此大的密码空间足以让人类计算机的总和望而却步。

4.3 弱密码字典

WPA-PSK 的密码空间用浩瀚来形容一点不为过，所以直接进行字典攻击是傻子的行为。但是作为一个密码对字典攻击来说有强密码和弱密码的区别。强密码就是破解希望极其渺茫的密码。弱密码是很有希望破解的密码。当然强弱也是个相对概念，他也是依赖于加安全制的。银行的密码一般都为 6 位。像这样密码空间如此小的密码。普通情况下都为弱密码。但是银行的 ATM 一天只让你试三次。三次密码不对锁卡。有这样的机制。6 位的就不再是弱密码了。由弱密码组成的字典叫弱密码字典。当然一般的弱密码有以下几种。

4.3.1 密码空间太小的密码

什么叫密码空间。密码可能字符个数为 n 密码的位数为 p 那么 n 的 p 次幂就是密码空间，例如一个 6 位数子的的密码他的密码空间 6M=10^6。密码空间的大小也是个相对概念，这个和安全体制有关系的。还有就是尝试密码的速度。在 WPA-PSK 的破解中。我们可以无限次的尝试。尝试密码的速度也和设备有关系。WPA-PSK 分布式破解无疑是用速度来换取同等时间里更大的密码尝试空间。在下面的攻击预算里会对这一部分内容做详细的补充。

4.3.2 社会工程学的弱密码

就是密码中带有一定的社会工程学属性。也就是说密码中带有和个人有关系的信息。这里列出一个 mm 做的社会工程学字典方便理解。

19602008.txt 1960-2008 年的生日组合
mydic.txt 自己弄的常用字典
abc-birth.txt 任意三字母＋所有的生日组合;
shouji10.txt 10 位的手机号
shouji11.txt 11 位的手机号
shouji.txt 上海的手机号
8－af16.txt 8 位的 abcdef 和 123456 的任意组合
8－qrafzv.txt qwerasdfz

当然你可以看到社会工程学字典中穷举法的影子。WPA-PSK 破解中一般情况下我们没有办法知道设置密码的人的具体信息。所以 WPA-PSK 破解就没法生成针对性很强的社会工程学字典。

4.3.3 有一定联系性规律性弱密码

例子：有人曾破如此一个 WPA-PSK 密码 IX1V7051242。如果你不了解这个密码的背景你肯能会觉得很神奇，这么强的密码也能破。这样的密码是在西班牙的 tele2 这样的 AP 上有,而且这样 AP_ESSID 里都有 tele2 字段。这样的密码后面的 8 位是相同的有真正的密码只有四位。四位密码其密码空间很小很容易被字典攻击出来。这个也是 AP 的默认密码。所以这个密码被破解是因为 AP 本身产生的随机密码就是个弱密码。是 AP 的厂家自己降低了安全性的做法。

4.3.4 暴露过的强密码

密码这个名字就告诉我们他是不能见光的。见光即死。见光的方式很多被偷窥了，被窃听了等。这里讲个典型点的例子：有些人具备一定的安全知识的。知道要设置一个密码空间很大的强密码如 acdess!@#$%，这个密码破之实在不易。但是这个 AP 的密码

还是被破解了。原因何在。因为这个人比较懒，他在任何地方都是使用的这个强密码。由此他注册了一个论坛。习惯性的输入自己的强密码。但是那个不怀好意的论坛的后台有个密码收集工具。他的密码被收录进字典。用这样的字典破他的 WPA-PSK 不是很容易吗。你是不是这样的人啊？至少我碰到一个就是他的 blog 密码和银行卡是一个密码。《剑鱼行动》中那个黑客是如何在一分钟进入国家安全信息网的啊。就是网络上工作着为他收集密码的程序。而他就是通过这样的字典迅速破解的。而这样的字典真正的黑客也是不愿意发布出来的。原因还是那句话密码见光即死。

4.4 强密码

看名字你就应该知道破解强密码的希望是十分渺茫的。怎么样的密码算一个强密码，第一肯定不能有上面弱密码的属性。第二是需要足够的密码空间。关于 WPA-PSK 中什么形式的密码可以被称之为强密码了，在下面的攻击预算里会指出来的。

5 攻击预算

拿分布式攻击来说。开始破解一个 WPA-PSK 包。我们知道他是 8 位的全字符一个密码。然后我们征集到万人自愿参加这个工作。可是一破破解了一周这个密码没有任何动静。这时人数减少了 50%，之后又破了一月，人数减少到 10%。这个 10%是很好的支持者，他们坚持数月。密码还是没有出现。这下就剩下 5%的绝对拥护者了。但是花开花又落密码还是没有出来。这时没有人在坚持了。这个密码最后还是没有被破解出来。那么我们的时间精力是不是都白花了呢。的确是这样。但是如果有这些人开始这个巨大的工程前，如果我们进行了预算。我们就会知道这 1 万个人即使进行全速破解这个密码，而且都是使用的 4 核心的处理器。那么他们也需要花上 27 年。看到这样的预算我想当时的 1 万人会有 99.9% 。还有 10 个人为什么不放弃。这还用问吗，他们都是愚公的子孙。很厉害的，山都能铲平。还搞不定你一个密码了。只要你的密码有限，而我的子子孙孙无穷匮也。攻击预算的意义就在此，提前让我们知道做这件事所需要的代价和所能获得的意义。不行进预算也是一种不成熟的表现。当然搞分布式计算的人可能知道这一点。他们早就强调分布式破解只是思路。不是破解方案。破不出来也没有关系。这样的人最可气，自己知道不可行也不说，害人误入歧途。空欢喜。

5.1 攻击预算的意义

预算运用的地方很广。迅雷下个大的电影他都会预算一下大概需要花多少时间完成这个任务。做大的工程预算更加不能少。字典攻击这样的常规攻击，理论上是能可行的但实际上不一定可行的。而攻击预算要解决的问题就是：在均衡了攻击代价后，攻击是否具有实际可行性？一般情况下攻击的代价主要是时间和资源。有强大的资源支持就可以节省时间(分布式破解就是走的这条路线)。当时间合适的话。而使用的资源远大于攻击带来的意义。那么这样的攻击也不具备现实意义。当然在一开始我用会使用极值的方式评估攻击方案的可行性的问题。即考虑最佳情况，如果还不行可以直接放弃。最差的情况，如果亦有可能值得深入。

5.2 WPA-PSK 中攻击预算

WPA-PSK 中的攻击预算是很容易的事。Aircrack 软件会告诉你详细的数据。让你进行攻击预算的。无论是你直接字典攻击还是建库都会明确的告诉你他的效率和所花的时间。而且他的数据是比较准确的。破解 WPA 是最好要在纯命令行下进行。在破解 WEP 的时候，由于现在计算机的速度比较快，你很难比较纯命令行模式和图形界面的执行的效率差异。但

是 WPA 字典攻击是及其耗费资源的。在命令行模式下会执行的更快。他们的速度差异是：命令行最快 398.24 k/s，windows 下次之 264.93 k/s， xwindwos 下最慢 158.95 k/s。像 linux 这么难用又 ugly 的系统，要不是他有惊人的执行效率。他早就淘汰了。所以破解 WPA 在纯命令行模式下有更高效的优势。下面是我在纯命令行模式下实测数据。

密码尝试数度 398.24key/s

产生 PMK 的速度是 193PMK/s PMK 库的增长数度是 24.6kb/s

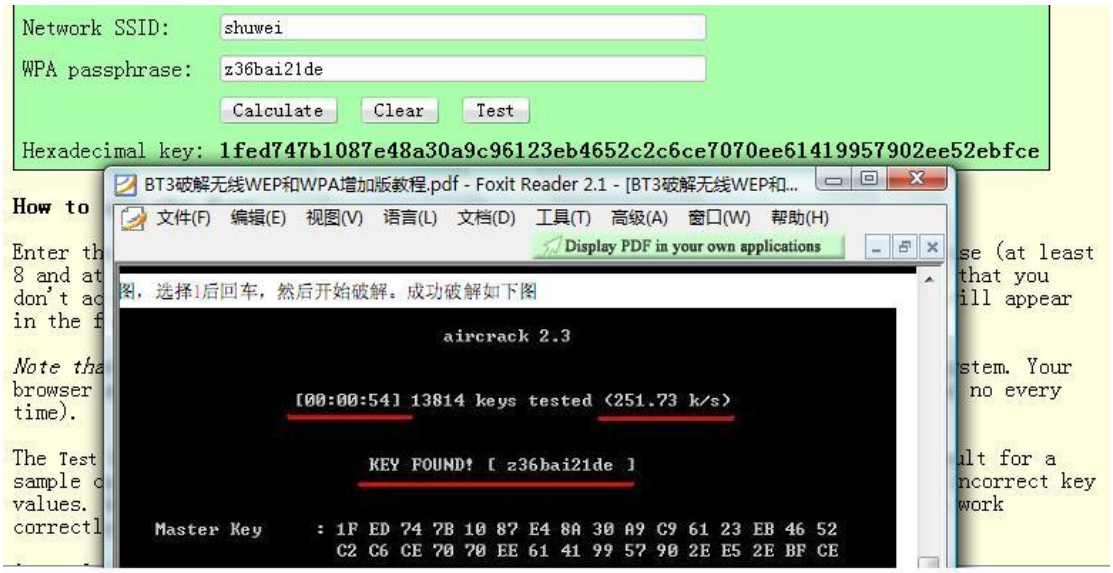
(没有想到吧 PMK 库的增长速度这么慢。还不如宽带快。)

直接 PMK 库尝试密码的速度为 57136.97key/s

也许你会说这是我计算机的上速度对其他计算机没有用。当然要通过上面的值换算成其他计算机的精确值是不行的。但作为估算是不需要进行精确换算的。那么性能不同的计算机一般是按什么指标换算其运算能力的呢？是按 GFLOPS（10 亿次扩展双精度能力/秒）。那些超级计算机等于多少台普通台式机不是实测出来的。也是通过上面的值进行换算出来的。我的计算机的这个数值是 10.3GFLOPS。如果你想转化成其他计算机的数值，只需要下载我提供的 EXCEL 表格他是会自动给你计算的。

5.3 WPA-PSK 中的隐蔽规则

上面你也看到我的密码尝试数度只有 398.24key/s。WPA-PSK 中曾经提及过设计者是知道字典攻击是唯一有效进攻 WPA-PSK 的手段。为此他也是在允许条件下对这一点严加防范。导致我的计算机尝试密码的速度只有这么点。他是如何防范的，四次握手生成 PMK 的函数 PSK=PMK=pdkdf2_SHA1(passphrase，SSID，SSID length，4096)，在这个函数里的输入值都很明了除了这个 4096。这就是设计者加入的防范。他的意思让函数迭代 4096 次。主要目的就是大大的降低字典攻击的效率。同时也增加了函数的复杂性。这个函数的消耗的时间占派生一个 MIC 的总时间的 99.3%。也就是 SHA1_PRF,HMAC_MD5 这两个函数消耗的时间只占不到总时间的 0.7%。看到这里你也该明白所谓的建库破解是怎么回事了。就是先完成时间上 99.3%的任务。产生一个 PMK 库。破解时只要完成时间上 0.7%的工作了。这也就解释了为什么建库比较慢。这里我们建的库叫 PMK 库。或叫 HMAC 预运算库。根本不是什么叫 Rainbow Hash 表。而且 PMK 的值还要经过那两个非线性的 HMAC 函数才是 MIC 值。我们建立的库怎么会有线性的特点。虽然建立了 PMK 库是提高了速度。但不要说线速破解。线速只有在按线性值排列了 Rainbow Hash 表里有。PMK 值根本没有按线性排列，也没有这个必要。排列他只会浪费时间，而起不到任何作用。如果要线速破解你还是去建立 MIC 值的线性库吧。这样能实现线速了。就是这个库只能对一个握手包有用。建立这样的线性库有意思吗。下面这个网站用 JAVA 实现了派生 PMK 的过程，和教程里的 PMK 相同吧。
http://www.xs4all.nl/~rjoris/WPAPSK.html



产生 PMK 如此费时，为什么硬件条件差的 AP 在握手时如此的迅速。实际是在你选择用 WPA-PSK 模式后。AP 就开始用密码和 ESSID 产生 PMK（WPA-PSK 初始化）以后他都保存了这个 PMK 值。除非你改 ESSID 或密码否则 AP 都不会花时间去生产 PMK。所以 STATION 和 AP 握手如此的快速。所以增大上面算法中 4096 的值只会增加初始化时间而，不会对握手和传输数据有任何时间上的影响。但是对攻击者就不同了，如果增大 10 倍那么字典攻击的速度就只有原来的 1/10 了。

5.4 隐蔽规则的作用

在 05 年的一片对 WPA-PSK 安全分析的文章上指出。对于一个安全的 WPA-PSK 密码当时最新 PC 也是没有希望破解的。当然 3 年过去了。一切都会变化。如今破解 WPA-PSK 的情况怎么样呢。首先我们例举一个密码，看看目前计算机的破解能力吧。这个密码是 8 位的全字符密码。当然我们选当今世界上能查到的最好的计算机进行破解。这个计算机叫走鹃浮点能力是 1.026PFLOPS。他穷举这个一个 8 位的密码，按照目前 WPA-PSK 的算法，需要 5 年时间。而破解密码至少要尝试一半的可能性。这样也需要 2.5 年的。而已上情况都是建立在那台超级计算机置国家安全于不顾。全力帮你破解密码的基础上的。你问我为什么不用库破解。8 位的全字符的穷举 PMK 库是 782PB。而那个超级计算机需要 10 年的时间才能建完这个库。而且这么个库跑一边也要花掉走鹃 13 天的时间。所以想模仿 Rainbow Hash 表在 WPA-PSK 中根本不现实。而 14 位的 Rainbow Hash 表有多大？走鹃目前的速度相当于 5 万台左右的个人 PC（四核）。但是分布式破解在 5 万台左右的个人 PC 上的表现肯定不如走鹃的。因为别人帮忙挂机时可能是下着电影看着高清进行的。也许你会说人多力量大。但是 08 年 500 强计算机的总和破解这样的密码也要花费 5.6 个月。所以该是时候认真考虑一下所谓分布式破解或建库的意义的时候了。

5.5 WPA-PSK 的强密码

刚才使用超级计算机极值估算的方式，我们知道了一个 8 位的全字符密码在 WPA-PSK 里可以称得上是一个强密码了。所以 WPA-PSK 的强密码第一没有上面弱密码的特性。第二满足下面的要求，使得密码有足够大的密码空间。

字符类型	等效密码长度(位)
10 位纯数字	15.82

26 位纯字母	11.18
36 位字母+数字	10.17
52 位大小写字母	9.22
62 位大小+数字	8.83
95 位全字符	8.00
HEX 密码长度	13.14

有些人爱抬杠。会说我上面列出的强密码也被破解过。我不否认有些人有心灵感应的潜能。别人设的强密码都设置到你的头脑里了，你不用破解直接知道密码。还有那种人是上帝的恩宠。别人再强壮的密码你的字典里都有的。如果你不是上面的两种人。如果你破了一周的密码还没有出来就放弃吧。你怎么就知道这个密码不是个强密码。有时还是需要理智放弃。网上破解 WPA-PSK 的教程很多。都是几分钟就破解的。有些密码还很强。教程吗都不是实战。都是知道密码在破密码。所以不要让那些教程误导了。以为破解 WPA-PSK 很容易。WPA-PSK 密码破解很长时间都不出来千万不要钻牛角尖。

5.6 WPA-PSK 的弱密码攻击

到现在我们明白了针对 WPA-PSK 的攻击目前唯一有实际价值的是弱密码字典攻击。由于弱密码攻击 WPA-PSK 的成功。就有人否定 WPA-PSK 的安全性。难道弱密码攻击就是 WPA-PSK 的安全性的弱点吗？这个例子可能大家都知道。一个人在旅馆里丢了钱包。钱包里有身份证、银行卡。结果银行卡里的前被盗了。原因是这个人用的是生日做的密码。而使用弱密码导致卡内资金被盗银行是没有责任的。同里所以你使用了弱密码 WPA-PSK 被破解 AP 和 WPA 的设计者都是没有责任的。在仅用密码保护的安全体系里，弱密码一项都是问题所在。我认为银行也不是一点责任都没有。信息高度敏感性的银行应该像网上的密码学习主动根据客户的信息判断是否为弱密码。发现弱密码该主动提醒客户并给客户补充安全知识。如果我们的 AP 也加入评估机制的话。破解 WPA-PSK 就更加雪上加霜了。那些说 WPA 漏洞百出的。你怎么不去说银行的系统不可靠呢。WPA 不会给你假币吧。但 ATM 会。

5.7 良好的弱密码字典

良好的弱密码字典对于破解 WPA 目前还是有一定作用的。但是由于以后安全措施的提高这样的字典最后也会失效。但是产生一个良好的弱密码字典并不是容易的。这样的字典需要收集很多的密码然后进行分析。最后总结出大众设置密码的特点。绝不是意想得来的。上面 mm 的字典不错，但是他如果知道他的字典普通的机器要跑一边要花上几个月的时间这个字典从时间上来看也太大了点。三跑两跑少女变老太了。而这么大的字典如同别人所说的手机号后面加个@这个字典就得挂。所以好的弱密码字典在于精而不在于大。而且上面的字典如此大传输也不方便。实际上面的字典也很容易压缩小。使用的时候完全可以边生成字典边破解。这就需要有个 linux 下工作的字典生成器了。配合这样的生成器字典就能变得很小了。700m 的字典需要 4～5 天的时间。而这样长的时间一般人也能接受。而且正好能刻个盘。比较实际。如果是 DVD 的字典需要 1.5 月才能跑完实用性也不强。

5.8 PMK 库的意义

PMK 的有点是速度，但为之牺牲的是漫长的建库时间，巨大的磁盘空间，SSID 的针对性也是 PMK 库的主要问题。所以 PMK 主要用于对付那种使用十分广泛的默认 SSID。一般陌生的 SSID 没有必要为他建立 PMK。还有 SSID 带有唯一性的。如新出的 TP-LINK。默认 SSID 变成了 TP-LINK+MAC 的前六位。这个做法无疑是想废了我们给 TP-LINK 做的 PMK 库。从另一个角度来说 TP-LINK 无疑是一个很注重安全的生产商。对于这样的 SSID 一般

不要为他生成 PMK 库。陌生的 SSID 为什么没有建立 PMK 库的必要。要么那个人不注重安全的他不会改密码。你破解了一次长期能用。要么他注重安全改个安全点的密码或有天他想个性化一下把 SSID 改成了他们家小狗的名字。任何一条导致我们辛苦建起来的库直接残废了。而唯一的用武之地就是别人不改 SSID，每次还改个你字典里有的弱密码让你破。所以为陌生的 SSID 建立 PMK 库意义不大。使用范围相当狭窄。精选 250m 左右的字典。这样单 SSID 的 PMK 库为 7G 一个 DVD 正好带的下。方便携带，也不会占用硬盘空间。这样一个 DVD 光盘普通计算机一半 30 分钟就能历遍了。这样的光盘对 WPA 的破解比较有实际意义。关于网络上的 SSID 库就没有那么有有用了。太大下了没有地方放。边下边破可以考虑，但是目前宽带满足不了 PMK 速率的要求。但是比直接的密码破解会快上几倍。

5.9 WPA-PSK 安全性

这里我们可以说 WPA-PSK 模式和一个强壮的密码配合完全能胜任安全要求比较高的场所。

6 结尾

与其把精力放在没有多少意义的分布式破解上，不如集中到下面。

配合 airodump-ng 的针对于 WEP/WPA-PSK 的窃听攻击。WEP 的窃听比较容易有密码就能随时任意窃听。WPA 的比较复杂。需要从握手开始窃听。并且在 WPA 有更新数据加密密码的机制。这样的窃听工具。就是把加密在 WEP 或 WPA 里的 IP 包解开来。有了这样的工具。我们可以很容易的解决关闭 HDCP 时陌生网段所使用的 IP 配置。也能从 IP 包里捕获明文帐号和密码了。如 AP 的登录密码。QQ 帐号等。科莱和 CAIN 也能完成上面的工作他们和窃听工具有什么区别。科莱和 CAIN 是通过 ARP 欺骗来获取数据的。这样捕捉的效率不如窃听工具。而且会使合法客户端链接不稳定。导致合法客户端使用了 ARP 绑定上面的攻击就无法使用了。窃听工具是工作在数据链路层的。在知道了密码的情况下这样的窃听防不胜防。如果那个高手把这样的工具弄出来告诉我一声哦。

梵音天

2008 年 9 月 23 日