ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.10, No.11, April 2014
E-mail: info@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

基于RC4算法IV脆弱性破解WEP秘密密钥

谢青松[1],汤玲[2],李甜[3],杜廷龙[1]

(1.西安通信学院,陕西 西安 710106;2. 61345部队,陕西 西安 710100;3. 61858部队,陕西 西安 710100)

摘要:在分析WEP协议加密原理的基础上,针对其核心RC4算法存在IV脆弱性的缺陷,给出了一种破解WEP秘密密钥的算法。该算法首先用无线数据帧的标识字段0XAA异或截获密文帧的第一个字节得到伪随机密钥序列的第一个字节,然后再根据截获的初始向量并利用RC4算法初始向量的脆弱性,计算出秘密密钥。实验结果表明,该算法能有效破解WEP协议的秘密密钥。

关键词:有线等效保密协议;RC4算法;初始向量的脆弱性

中图分类号:TP311 文献标识码:A 文章编号:1009-3044(2014)11-2517-03

Crack WEP Secret Key Based on IV Weakness of RC4 Algorithm

XIE Qing-song[1], TANG Ling[2], LI Tian[3], DU Ting-long[1]

(1. Xi'an Communication Institute, Xi'an 710106, China; 2.61345 Troops, Xi'an 710100, China; 3. 61858 Troops, Xi'an 710100, China)

Abstract: This paper presents a algorithm used to crack WEP secret key on the base of analyzing the theory of WEP, according to the bug of RC4 algorithm which is the core of WEP. Firstly, this algorithm gets the first byte of pseudo random secret key sequence by XORing the identification filed of wireless data frame 0XAA and the first byte of captured secret frame. Secondly, this algorithm calculates the secret key, according to the IV Weakness of RC4 algorithm and the initialization vector of the wireless data frame. The experimental result shows that the proposed algorithm can effectively crack WEP Secret Key.

Key words: Wired Equivalent Privacy; RC4 algorithm; IV Weakness

802.11无线网络采用有线等效保密WEP(Wired Equivalent Privacy)协议来为无线网络中的数据通信提供机密性和完整性保护。然而WEP协议存在缺陷,攻击者可以破解WEP协议的密钥,这给无线通信带来安全隐患[1]。该文首先分析了WEP协议的加密原理,然后详细分析了WEP协议的核心RC4算法及其存在IV脆弱性的缺陷,最后针对该缺陷给出了破解WEP秘密密钥的详细步骤。

1 WEP协议

WEP协议由认证协议和加密协议组成。认证协议用于确认通信双方的身份,加密协议用来确保通信数据的秘密性。WEP加密协议的基本原理如图1所示[1]。

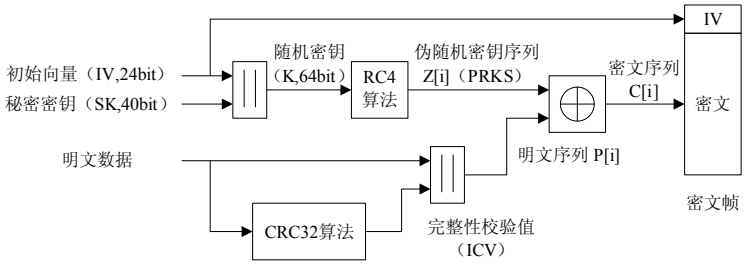

图1 WEP协议的加密原理

WEP协议加密的过程分为四步:首先,将用户输入的秘密密钥和随机生成的初始向量IV(Initialization Vector)拼接成密钥;然后将此密钥作为RC4算法的输入产生伪随机密钥序列;其次将明文数据及其完整性校验值的组合作为明文序列;最后,用伪随机密钥序列异或明文序列的结果作为密文序列,并将初始向量IV和密文序列的组合作为密文帧发送给接收方。解密的过程与此类似。

收稿日期:2014-02-23
作者简介:谢青松(1982-),男,四川苍溪人,讲师,硕士,主要研究方向为网络安全。

从WEP协议的加密原理框图中可以看出两点：初始向量IV以明文的方式进行传输；WEP加密协议的核心是RC4算法。但由于RC4算法存在固有缺陷，易受IV Weakness攻击，进而攻击者可以完全恢复出WEP协议的秘密密钥。

2 RC4加密算法

RC4加密算法是Ron Rivest在1978年设计的密钥长度可变的流加密算法簇。RC4算法由两部分组成：密钥调度算法KSA（Key Scheduling Algorithm）和伪随机密钥序列生成算法PRGA（Pseudo Random Generation Algorithm）。密钥调度算法KSA将输入 L 字节的随机密钥 K 生成一个由 N 个元素组成的排列 S，L 一般为8或16，N 一般为256。伪随机密钥序列生成算法PRGA由密钥调度算法产生的随机排列 S 产生伪随机密钥序列 Z。

记密钥调度算法KSA中循环进行 i 次后随机排列 S 的状态为 $s_i(i=-1,0,1,\cdots,N-1)$，s_{-1} 表示第一次循环之前排列 S 的状态。对于某个 i，记 $X=s_i[1]$，$Y=s_i[X]=s_i[s_i[1]]$，则 $Z=S_i[X+Y]=S_i[S_i[1]+S_i[S_i[1]]]$，如图2所示。

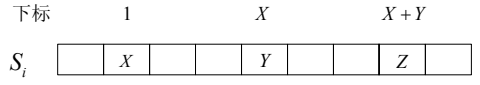

图2 RC4算法中密钥调度算法产生的随机排列 s_i

记Swap(S[i],S[j])表示交换排列S中下标为i和j的元素。如果将密钥调度算法KSA循环中的“Swap操作”看做真随机，那么约有5%的概率X，Y，Z三个元素都不会在第 i 次循环之后的“Swap操作”中出现，进而 $Z=S_i[X+Y]=S_i[S_i[1]+S_i[S_i[1]]]$ 将是RC4算法输出的第一个伪随机密钥字节[2]。这就是RC4算法的缺陷，即IV Weakness缺陷。

3 基于IV Weakness破解WEP秘密密钥

在WEP中，K[0]、K[1]和K[2]是以明文方式传输的IV，攻击者希望得到的是秘密密钥K[3]、K[4]…。为了得到K[3]，可以构造一种特殊格式的IV（3，N−1，x），其中x为任意值。下面我们来跟踪KSA的执行过程[3]。

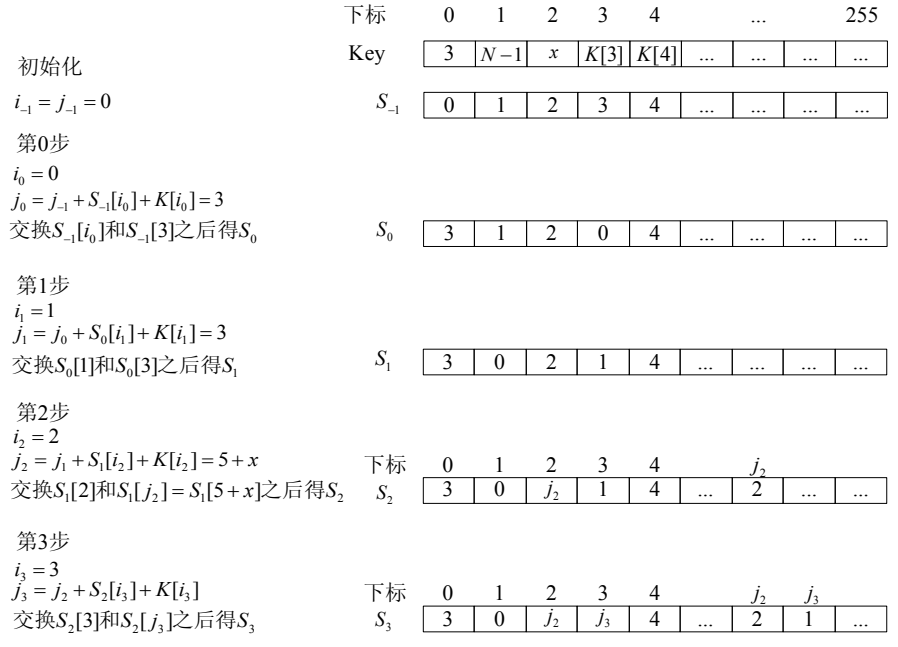

图3 密钥调度算法的执行过程

在状态 S_3 中，令 $X=S_3[1]=0$，$Y=S_3[X]=3$，则 $Z=S_3[S_3[1]+S_3[S_3[1]]]=S_3[X+Y]=S_3[3]$。有5%的概率，$X$，$Y$，$Z$ 三个元素都不再参加其后KSA中任意一次Swap操作，即有5%的概率PRGA输出的第一个字节为 $Z=S_3[3]$。由于 $S_3[3]=S_2[j_3]$，因此攻击者可以从已知的 S_2 中搜索出一项其值为 Z，找到该项对应的位置下标 j_3。又因为 $j_3=j_2+S_2[i_3]+K[i_3]=j_2+S_2[3]+K[3]$，可以反推出 K_3 的估计值。当 $X(3,N-1,x)$ 中 x 取不同值时，重复上述步骤可以得到大量 $K[3]$ 的估计值。其中，出现次数最多的那个估计值是 $K[3]$ 的真实值的可能性最大。

考虑一般情况，在已知 $K[0]$，$K[1]$，$K[2]$，…，$K[A+2]$ 的情况下，如何得到 $K[A+3](A=0,1,2,\cdots)$ 的值。攻击者可按下述步骤进行破解。

1) 攻击者利用自己计算机中设置为混杂模式的无线网卡观察无线网络中正在发送的密文帧，对含有满足 $(A+3,N-1,x)$ 形式IV的密文帧进行捕获，并记录该密文帧的第一个字节 $C[1]$。

2) 用捕获密文帧的第一个字节 $C[1]$ 异或无线数据帧的标识字段0XAA，得到密钥流的第一个字节 $Z[1]$。该字节为PRGA输出的第一个字节。

3) 攻击者自己构造特殊格式的初始向量 $IV(A+3,N-1,x)(A=0,1,2,\cdots)$，并执行KSA运算到第 $A+2$ 步，得到 j_{A+2}，S_{A+2}。

4) 在 S_{A+2} 中搜索出值为 $Z[1]$ 的元素，找到该元素的位置下标 j_{A+3}。

5) 根据 $j_{A+3}=j_{A+2}+S_{A+2}[A+3]+K[A+3]$，可得 $K[A+3]=j_{A+3}-j_{A+2}-S_{A+2}[A+3]$，由此得到 $K[A+3]$ 的一个估计值。

6) 攻击者继续捕获初始向量 $IV(A+3,N-1,x)$ 中 $x=0,1,2,\cdots,255$ 时的密文帧，重复第(2)至第(5)步，得到256个 $K[A+3]$ 的估计值，取出现次数最多的那个估计值作为 $K[A+3]$ 的最终估计值。

4 实验结果

破解WEP秘密密钥的实验环境由一台无线接入点、两个客户端和监听者组成，如图4所示。

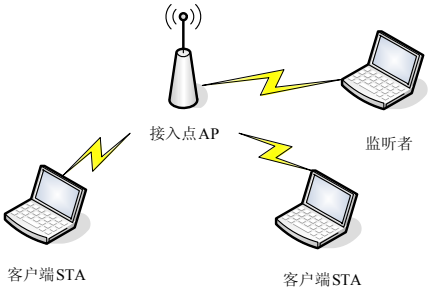

图4 破解WEP秘密密钥的实验环境

```
bt ~ # aircrack-ng -x -f 2 ciw.cap-02.cap
Opening ciw.cap-02.cap
Read 42250 packets.

   #  BSSID              ESSID                     Encryption

   1  00:0B:B5:EE:3F:D9  default                   WEP (41601 IVs)

Choosing first network as target.

Opening ciw.cap-02.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 41601 ivs.
                      KEY FOUND! [ 12:34:56:78:99 ]
       Decrypted correctly: 100%
```

图5 破解WEP秘密密钥的结果

接入点是Linksys WRT54G2无线路由器，支持802.11b/g/i协议。客户端使用的计算机安装华硕WL_167G无线网卡。监听者使用的计算机安装华硕WL_167G无线网卡，同时安装有基于上述破解原理编写的破解程序。

监听者首先截获大量的无线数据帧，然后根据上述步骤破解WEP秘密密钥。破解结果的界面如图5所示，可以看出，成功破解的秘密密钥为“1234567899”。

5 结束语

利用WEP协议核心RC4算法存在IV Weakness的缺陷，根据捕获的无线密文帧及其明文标识字段0XAA，提出了破解WEP秘密密钥的算法。实验结果表明，在获取大量无线数据帧的情况下，该算法能有效破解WEP协议的秘密密钥。

参考文献：

[1] 曹秀英,耿嘉,沈平.无线局域网安全系统[M].北京:电子工业出版社,2004.

[2] Stubblefield A, Ioannidis J, Rubin A.D. Using the Fluhrer, Mantin and Shamir Attack to Break WEP[R].AT&T Labs Technical Report, 2001.

[3] Fluhrer S, Mantin I. and Shamir A, Weaknesses in the key scheduling algorithm of RC4 [EB/OL]. http://www.drizzle.com/aboba/IEEE/rc4_ksaproc.pdf.

(上接第2516页)

参考文献：

[1] 陈淑英.无线光通信技术综述[J].广西通信技术,2010(1).

[2] 麦结容.刍议无线光通信传输与接入[J].华东科技:学术版,2013(10).

[3] 崔桂海.浅析无线光通信传输与接入[J].中国新通信,2013(20).

[4] 王璐,张在宣,余向东,刘玉衡,张字飞.无线光通信宽带接入技术及其应用[J].光电子技术与信息,2010(6).