无线局域网协议 802.11 安全性分析

孙 宏,杨义先
(北京邮电大学信息安全中心,北京 100876)

摘 要: 本文从身份认证、通信的机密性、完整性和不可否认性方面对 IEEE 无线局域网协议 802.11 的安全机制进行分析,证明了该协议的安全机存在着严重的安全漏洞,实际上该协议的安全机制无法保障无线局域网的安全通信. 本文还指出了实际中可能存在的攻击,针对文中提到的漏洞和可能受到的攻击,提出了相应的解决方案.

关键词: WEP; 认证; 共享密钥; 密钥流; RC4
中图分类号: TP393.1 **文献标识码**: A **文章编号**: 0372-2112 (2003) 07-1098-03

On the Security of Wireless Network Protocol 802.11

SUN Hong, YANG Yi-xian
(Information Security Center, Beijing Univ. of Posts & Telecomm, Beijing 100876, China)

Abstract: This article focuses on analyzing the security mechanism of IEEE Standard 802.11. It is proved in this article that there are many security holes existing in the security mechanism, which is not immunized from the malicious attack. And in view of authentication, privacy, integrity and nonrepudiation, the security mechanism is unable to ensure the security of the WLAN telecommunication. Proper solutions are proposed to overcoming the weakness of the security mechanism.

Key words: WEP; authentication; shared key; key stream; RC4

1 引言

随着笔记本电脑、掌上电脑等移动终端的普及,无线局域网的应用以其接入的灵活性,架构及扩展的方便性得到了迅速增长. 但是由于基站 STA(Station)之间传送的信息都暴露在空气中,这使得机密信息的窃取变得更加容易,信息的泄漏也更加容易. 无线网络的信息安全是一个不容忽视的重要环节.

根据无线局域网协议 802.11[1],无线局域网的安全是通过 WEP(Wired Equivalent Privacy)[1]来实现的. 802.11 的安全机制由认证、加密和数据的完整性三方面构成. 802.11 的服务群体分为两类:一类是 IBSS(Independent Basic Service Set),另一类是 BSS. 在 IBSS 中,每个基站都是对等的,可以直接进行通信,基站与 IBSS 的外部进行通信时则需经过网关;在 BSS 中,基站之间的通信或者基站与外界用户进行通信都必须经过 BSS 中的访问点 AP(Access Point),先与 AP 进行认证,建立联接,然后才能继续进行通信. 由于 BSS 的认证机制更加完善,而且 IBSS 和 BSS 的加密机制是相同的,所以,下面的论述就以 BSS 为基础. 802.11 的认证过程和保密通信都应用了 WEP 算法,在 WEP 基础上进行了访问控制(认证)和数据加密,目的是提供具有与有线网络的安全级别等同的安全机制,有效地防止信息泄漏. 下面通过对 WEP 实施过程的各个环节进行安全性分析,指出其中的安全漏洞,描述了实际中可能存在的安全攻击,提出了解决上述问题的一些设想及方案.

2 认证的安全问题

在 802.11 协议中,基站之间的认证是通过判断对方是否拥有共享的密钥 K 来进行的. 在认证的过程中用到了 WEP 算法. 分析证明,该认证方式很容易受到已知明文攻击[2].

2.1 认证的过程

(1) 被认证方 STA 向 AP 发送认证请求.

(2) AP 向 STA 发送挑战信息 P,该挑战信息是由 WEP 的伪随机序列发生器 PRGN 采用 $RC4$[2] 算法生成的随机序列(长度固定为 128 字节).

(3) STA 使用 WEP 算法加密挑战信息,也就是说首先计算 P 的校验值 $ICV(P)$,然后用初始向量 IV 与共享密钥 K 相连接作为 PRGN 的种子密钥,经过 RC4 得到加密用的长度与 $P \| ICV(P)$ 相同的加密密钥流 $S(S = \mathrm{RC4}(IV \| K))$,然后与 $(P \| ICV(P))$ 按 bit 进行 XOR 运算,得到密文 C,最后将 $(IV \| C)$ 发送给 AP. 此处以及下文中的符号"‖"表示连接.

(4) AP 用共享密钥 K 及接收到的 IV 生成密钥流,解密 C 得 $(P' \| ICV')$. 首先,AP 判断 $ICV' = ICV(P')$ 是否成立,如果不成立则认证失败,如果等式成立,则继续判断 $P' = P$ 是否成立,如果成立,则认证成功,否则认证失败.

2.2 安全性分析

由于认证者向被认证者发送的挑战信息是以明文形式传送的,非法用户在第二步可以监听到这部分信息 P,在第三步可以得到加密后的密文 C,只需计算出 P 的校验值 $ICV(P)$,就可以得到 $P \| ICV(P)$,然后把这个结果与监听到的密文 C 进行简单的异或运算就可以得到加密用得密钥流 $S:(P \| ICV(P)) \oplus C = (P \| ICV) \oplus ((P \| ICV) \oplus S) = S$. 由于 BSS 中的各个 STA 以及 AP 是共享密钥 K 的,而且 K 在一定的时间内是不变的,因此,攻击者一旦得到某个 IV 对应的密钥流 S,那么他就可以监听数据包的 IV 值,当相同的 IV 出现时,他就能够解密得到对应的明文. 以此类推,攻击者可以用这个漏洞建立起每一个 IV(共有 2^{24} 个,IV 在 WEP 帧中占 3 个字节)与其

收稿日期:2002-02-26;修回日期:2002-11-18
基金项目:国家重点基础研究发展规划(No. G1999035805);国家杰出青年基金(No. 69425001);国家自然科学基金(No. 60073049)

对应的密钥流 S 的码表,这样他就能够伪装成合法用户,用相应的密钥流正确加密 AP 送出的任意的挑战信息,从而得到 AP 的认证;或者能够解密用相同的共享密钥加密的长度为 128 字节所有的消息.

3　数据加密的安全问题

802.11 中数据的机密性是通过 WEP 算法进行加密来实现的.由于 WEP 的加密机制采用的是流密码,数据的机密性取决于密钥流的安全性.如果能够使得加密每个数据包的密钥流都互不相关,那么这种加密方式将是安全的.

3.1　IV 冲突

在 WEP 中,IV 与共享密钥 K 联在一起构成 PRNG(RC4)的 8 字节种子密钥,经过 RC4 产生用于加、解密的密钥流.其中,种子密钥的前 3 字节是 IV,后面的 5 字节是共享密钥 K.K 在一定的时间内是不变的,因此密钥流的变化依赖于 IV 的变化,换句话说,如果 IV 不变,经过 RC4 后得到的密钥流也不会变.当两个 WEP 帧的 IV 相同时,由于加密运算是密钥流与明文的简单的异或,这很容易受到已知明文攻击:

$$C1 = P1 \oplus \mathrm{RC4}(IV \parallel K)$$
$$C2 = P2 \oplus \mathrm{RC4}(IV \parallel K)$$

则
$$C1 \oplus C2 = P1 \oplus \mathrm{RC4}(IV \parallel K) \oplus P2 \oplus \mathrm{RC4}(IV \parallel K) = P1 \oplus P2$$

如果攻击者已知其中之一比如 $P1$,那么他很容易获得另外的一个明文 $P2$ 的全部(当 $P1$ 的长度大于等于 $P2$ 的长度)或部分(当 $P1$ 的长度小于 $P2$ 的长度).即使攻击者不知道有关明文任何信息,由于一般情况下传送的信息都是有冗余的,他可以根据字符出现的频度等等信息猜测出明文的内容;还有通过模式识别,攻击者也能够分辨出两个明文[3].况且,攻击者可以计算明文的 ICV 值,与恢复的 ICV 值相比较,如果结果一致,就证明他恢复的明文是正确的.另外,如果攻击者知道对应某个密文的明文,那么他很容易获得相应的密钥流,通过监听 IV,他可以获得所有用该密钥流加密的明文(假设这期间密钥 K 没有变化).

802.11 建议每一个 WEP 帧的 IV 都不同.从 IV 的长度可以看出,IV 实际上只有 2^{24} 种可能值,也就是说,在 K 不变的情况下 PRGN 最多能够产生 2^{24} 个不同的密钥流.我们知道,利用生日攻击[2],两个数据包具有相同的 IV 的概率为 $p_2 = 2^{-24}$,第 $n(n \geq 3)$ 个数据包的 IV 与前面产生的 $n-1$ 个数据包的 IV 有重合的概率为 $p_n = p_{n-1} + 2^{-24}(n-1)(1-p_{n-1})$.这样,如果按照无线局域网的理想流量 11Mbps 计算,那么仅仅在 1、2 秒之后 IV 的重复概率就会达到 99%[4].另外,在实际系统当中,许多厂家在 IV 的产生办法上没有过多地投入力量,大多数都采用 IV 经过固定的时间段变化或者是通过计数的方法给每个数据包赋值.对于前一种方案,很有可能会造成连续发送的几个数据包的 IV 值是相同的;而后者则往往采取初始化时 IV 的初值赋 0,这样,如果系统经常进行初始化,那么,小数的重复概率会大大高于大数的重复概率.这两点都显然会被攻击者利用的.24bit 的 IV 空间对于安全来说显然太微不足道了.实际上,通过以上的分析,即使 IV 的空间加大,WEP 对于已知明文攻击和选择密文攻击仍然是无能为力的.

3.2　WEP 的帧结构

WEP 的帧结构形式影响到了 RC4 的安全.在 802.11 中,RC4 的密钥是由 24bit 的 IV 和 40bit 的共享密钥连接而成的.并且 IV 是不经过任何加工传送给接收方的,也就是说 RC4 的部分密钥是暴露给攻击者的.当共享密钥不变,通过收集大量的 IV 值,及相应的 RC4 产生的密钥流的前面几个字节,攻击者就能够导出这部分的共享密钥[5].在实际的系统中,大多采用计数器来产生 IV 值,这样使得不同数据包的 IV 具有很强的相关性,因此也为攻击者提供了方便.

4　数据完整性校验的问题

802.11 规定,接收数据的完整性校验是通过校验函数 CRC-32 来实现的.要加密的明文 P 经过 CRC-32 算法得出一个校验和 ICV,然后 P 与 $ICV(P)$ 联在一起经过加密传送给接收者.在接收端,接收者解密密文得到明文 P' 和 ICV',然后,接收者计算 P' 的校验和 $ICV(P')$,如果 $ICV(P') = ICV'$,就认为恢复的明文 P' 就是没有经过篡改的原始的明文 P;反之,认为该数据包遭到破坏,于是抛弃该数据包.通过下面的论述可以看到,CRC-32 虽然能够检测出在传输过程中随机发生的差错,但是它不能检测出恶意篡改.

4.1　更改密文

由于 CRC-32 是线性函数,对于 $x \oplus y$ 有:$ICV(x \oplus y) = ICV(x) \oplus ICV(y)$.在不知道明文的情况下,攻击者就可以任意地更改密文,而不被发现.比如,攻击者想更改密文 C 的某些位,他可以通过 $C \oplus (x \parallel ICV(x))$ 来实现(其中,x 对应着 C 的改变位的位置取 1,其余位取 0).

攻击者篡改密文:

$$\begin{aligned} C' &= C \oplus (x \parallel ICV(x)) \\ &= (\mathrm{RC4}(IV \parallel K) \oplus (P \parallel ICV(P))) \oplus (x \parallel ICV(x)) \\ &= \mathrm{RC4}(IV \parallel K) \oplus (P \oplus x) \parallel (ICV(P) \oplus ICV(x)) \\ &= \mathrm{RC4}(IV \parallel K) \oplus (P \oplus x) \parallel ICV(P \oplus x) \end{aligned}$$

接收端解密:

$$\begin{aligned} &\mathrm{RC4}(IV \parallel K) \oplus C' \\ &= \mathrm{RC4}(IV \parallel K) \oplus RC4(IV \parallel K) \oplus (P \oplus x) \parallel ICV(P \oplus x) \\ &= (P \oplus x) \parallel ICV(P \oplus x) \\ &= P' \parallel ICV(P') \end{aligned}$$

因此,通过以上的处理,攻击者可以任意地篡改密文的某些位,从而达到改变明文的某些位的目的,但是接收者却不能通过取整校验来检测到这一动作.

4.2　借助 AP 得到明文

攻击者通过前述方法,可以通过更改加密的数据包的 IP 目的地址,把原来的 IP 目的地址改变为自己的 IP 地址,而不被 AP 检测出来.这样,数据包在 AP 被解密后,由 AP 将解密后的数据包送到攻击者处,攻击者就会轻而易举地得到明文.

5　建议改进措施

通过以上的分析可以看出,802.11 的安全漏洞主要反映在认证的不安全性,数据校验的非机密性以及采用流密码时产生的密钥流的相关性上.下面主要从这三个方面讨论一下

如何有效地改进 802.11 的安全机制.

5.1 身份认证

身份认证首先应该是双向的,建立联合时既要有 AP 对 STA 的认证又要有 STA 对 AP 的认证,前者保证了用户 STA 的合法性,后者保证了 AP 的真实性.其次,身份认证应该基于被认证方的多个特征,如:MAC 地址、SSID、共享密钥、用户的口令等等,这样不仅能够增加非法用户攻击的难度而且能够进一步保护被认证用户.另外,STA 与 AP 的认证密钥与会话密钥相同而且在相当长的时间周期内稳定不变,这严重影响了系统的安全性,如果会话密钥能从认证的交互信息中导出或在认证成功时由可信赖的第三方配给,就能解决这个缺陷.

按照上述的思想,基于现有的协议和标准,可以借助于网络端口访问控制标准 IEEE802.1X[6]实现 WLAN 的认证和密钥分配.IEEE802.1X 是一种安全标准,为 IEEE802 局域网提供认证和授权机制.

5.2 数据加密

IV 的重复使用导致相同的密钥流重复使用是 802.11 的 WEP 加密方案的主要问题之一.针对这一问题,WEP2 加大了 IV 的长度,为 128 比特.这虽然大大降低了 IV 的重复概率,但是通过前面的分析可以看出这不能从根本上解决问题.

设想把共享密钥与会话对应起来,也就是说在每次会话时 STA 向 AP 申请认证,得到一个新的共享密钥(会话密钥),将会话数据分成固定长度(比如 16 个字节)的 n 段 MPDU,并依次分配 0 到 $n-1$ 的序号.这个序号就是 IV 的值,IV 与共享密钥联在一起作为 *RC*4 的密钥种子,得到的随机序列丢弃前两个字节(以增加攻击 *RC*4 的难度),然后按照 802.11 的 WEP 算法进行加密.这样由于不同会话对应不同的共享密钥,而每个会话分割成的 MPDU 的 IV 与 0 到 $n-1$ 的数字一一对应,这样就保证了不会有重复的密钥流的产生,能有效地抵御字典攻击和密钥重放攻击.

即使解决了 IV 冲突以及密钥流的重复出现的问题,也不能改变 WEP 算法的缺陷——过于简单,不能抵御已知明文攻击.解决这个问题就是采用新的更加安全的算法来代替 WEP,比如说 3DES、AES-OCB 等等.3DES 是比较成熟的算法,易于硬件实现,AES-OCB 是一个比较新的算法,倾向于软件实现,而且其安全性有待考验.负责 802.11 安全策略的 IEEE 802.11 TGi 工作组在今年三月提交的草案中把 AES-OCB 作为 802.11 的新的加密算法.

5.3 数据完整性检验

由于 *CRC*-32 只能检测传输中出现的差错,对于恶意篡改无能为力,这里除了用 *CRC*-32 对接收到的数据进行校验外,用 HMAC-SHA1[7]对会话数据进行散列运算,所用的密钥可以同加密密钥一起在认证的过程中分配.具体过程如下:

(1)发送方用 HMAC-SHA1 对会话数据进行散列计算,得到的散列值与会话数据联在一起;

(2)然后将这部分数据按照 5.2 节所述进行分段成 MPDU,并由 *CRC*-32 计算出响应的 ICV 值,将 ICV 值与 MPDU 联在一起进行相应的加密后发出;

(3)接收方将收到的数据包解密,首先根据每个数据包的 ICV 判断是数据是否被破坏,如果 ICV 值不一致,则丢弃该数据包,并通知发送方;

(4)如果每个数据包的 ICV 校验都通过,接收方根据 MPDU 的序号将 MPDU 重新组合在一起,将除散列值之外的数据进行 HMAC-SHA1 计算,如果得到的散列值与接收到的散列值相等,则可以认为数据是由发送方发过来的没有被篡改的数据,否则丢弃该数据.

由于 HMAC-SHA1 算法必须在密钥的参与下进行计算,攻击者即使通过前述攻击手段更改数据内容而不被 *CRC*-32 算法检测出,但是由于不知道 HMAC-SHA1 的密钥,就无法计算出改动后的内容的散列值来替换原文的散列值,就达不到欺诈的目的.

6 结束语

以上论述了无线局域网协议 802.11 所存在的一些安全问题,并且有针对性地提出了解决方案.WLAN 的安全不仅仅靠 802.11(只提供 MAC 和 PHY 的安全)来实现,还需要高层安全协议和安全技术的配合.比如说在第二层利用 802.1X 进行认证和密钥分配,在第三层应用 VPN/IPsec 技术等等.但是这些协议的有效应用不是简单的堆砌,如何使这些高层的安全策略和 802.11 的安全机制有效地的结合,是目前亟待解决的问题.

参考文献:

[1] ISDN0-7381-1812-5. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications ANSI/IEEE Std 802.11 [S].

[2] Bruce Schneier. Applied Cryptography [M]. USA: Wiley, 1997.

[3] E Dawson, L Nielsen. Automated cryptanalysis of XOR plaintext strings [J]. Cryptologia, 1996, (2): 165 - 181.

[4] N Borisov, L Goldberg, David Wagner. Intercepting mobile communications: The insecurity of 802.11 [A]. Proc of 7th Annual Int. Conf. Mobile Computing and Networking 2001 Papers [C]. Rome, Italy: ACMCN, 2001.

[5] S Fluhrer, I Mantin, A Shamir. Weaknesses in the key scheduling algorithm of RC4 [A]. Preliminary Draft [C]. Canada: CRYPTO, 2001.

[6] ISDN0-7381-2927-5. IEEE Standard for Local and Metropolitan area networks——Port-Based Network Access Control, IEEE Std 802.1x-2001 [S].

[7] Krawczyk H, Bekkare M, Canetti R. HMAC: Keyed-Hash for Message Authentication [Z]. RFC 2104, February 1997.

作者简介:

孙 宏 女,1972 年 9 月生于山东平度市,1994 年毕业于解放军信息工程大学通信工程系,2000 年在该校获工学硕士学位,现为北京邮电大学信息安全中心博士研究生,研究方向为电子商务的安全技术.

杨义先 (见本期第 1045 页)