无线局域网WEP安全机制的研究

张 韬[1,2]

（1.湖南工业大学，湖南 株洲 412007；
2.武汉理工大学 信息工程学院，湖北 武汉 430070）

摘 要：WEP协议是IEEE802.11标准规定的数据加密机制，虽提供了64位和128位的密钥机制，但仍然存在许多缺陷。详细分析了WEP的工作原理，并说明了WEP存在的安全问题，最后讨论了相应的解决方案。

关键词：无线局域网；网络安全；IEEE 802.11；WEP
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673-9833(2009)01-0058-00

Research on Security Mechanism of Wireless Local Area Network's WEP

Zhang Tao[1,2]
(1. Hunan University of Technology，Zhuzhou Hunan 412007，China；
2. School of Information Engineering，Wuhan University of Technology，Wuhan 430070，China)

Abstract：With the standard regulation of IEEE 802.11 wireless local area network, the security issues become more and more noticeable. WEP algorithm is the data encryption technology prescribed IEEE 802.11, which provides 64 bit and 128 bit key mechanisms but still has many limitations. The working principle of WEP is analyzed and the secure troubles are also narrated. Finally, its corresponding solving project is also discussed.

Key words：wireless local area network; network security; IEEE 802.11; wired equivalency privacy

0 引言

无线局域网络通讯信号裸露在空气中的特点带来了比有线网络更多安全威胁的问题。1999年11月，由LAN/MAN标准委员会下属的无线工作组制定了IEEE 802.11无线局域网标准。此标准针对安全问题规定了2部分机制：一是访问认证；二是数据加密，即WEP（Wired Equivalency Privacy，有限对等加密机制）[1]。如今，这2种机制已成为了无线局域网系统中安全机制的主要形式和基础。对于这2种机制来说，前者仅提供简单的访问控制，比较低级；而WEP协议采用了基于RC4算法的数据加密技术，以满足用户更高层次的安全需求，从而得到了广泛的应用。但WEP并没有达到人们的期望，相反由于其设计上的失误，使得WEP本身存在着致命的漏洞。

1 WEP算法的工作原理

WEP的作用有2点：1）明文数据的加密；2）保护未经认证的传输篡改。

由于IEEE 802.11协议的设计思想是尽可能模拟有线局域网，并对上层保持透明，所以WEP并不试图保证端到端的安全性，而仅仅保证从无线站到接入点AP间传输链路的安全。

1.1 WEP算法加密后的数据帧格式

WEP通过发送方和接收方共享的密钥K来保护通讯双方交换的数据部分。允许无线站与AP最多共享4个WEP用户密钥。具体使用哪个WEP用户密钥由WEP帧中的KeyID决定，图1显示了WEP帧的结构。

收稿日期：2008-11-14
作者简介：张 韬（1979-），男，湖北襄樊人，湖南工业大学讲师，武汉理工大学硕士生，主要研究方向为网络技术，信息安全，E-mail：ztchina0070886@Sina.com

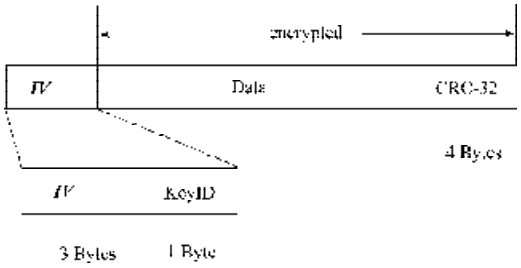

图 1　WEP 帧格式

Fig. 1　WEP encrypted frame

1.2　WEP 加密过程

WEP 依赖通信双方共享的密钥来保护传输的加密帧数据。WECA（Wireless Ethernet Compatibility Alliance）组织要求通过 Wi-Fi 认证的 WLAN 产品都必须支持至少 40 位的 WEP 加密协议[2]。其加密数据帧的过程如下：

1）计算校验和（checksumming）。首先根据消息 M 计算完整校验和 $c(M)$，将 M 和 $c(M)$ 连接得到明文 $P=[M, c(M)]$；

2）加密。在这个过程中，将第 1）步得到的明文采用 RC4 算法加密，如图 2 所示。

选择 1 个 24 位的初始化向量 $V(IV)$。RC4 算法用 V 和共享密钥 K 产生 1 个 64 位的密钥流，即 1 个长的伪随机字节序列 PRNG（pseudo random number generator）。然后，将明文与密钥流进行按位异或操作 XOR（记为 ⊕），得到加密的信息，即密文：$C=P \oplus \mathrm{RC4}(V, K)$；

3）传输。将 V 和 C 串接得到传输的加密数据帧，在无线链路上传输。

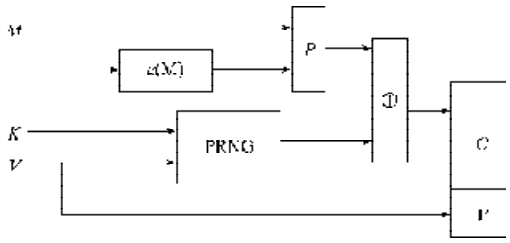

图 2　WEP 加密流程

Fig. 2　WEP encryption process

1.3　WEP 解密过程

解密过程只是加密过程的简单取反，如图 3 所示。

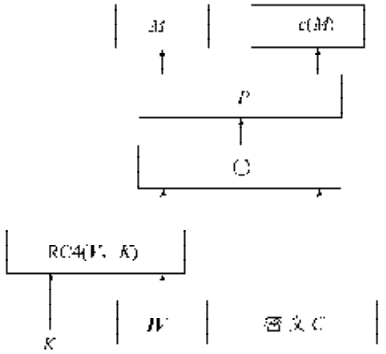

图 3　WEP 解密流程

Fig. 3　WEP decryption process

1）恢复初始明文。重新产生密钥流 RC4(V, K)，将其与接收到的密文信息进行异或运算，以恢复当初的明文信息；

2）$P'=C \oplus \mathrm{RC4}(V, K)=(P \oplus \mathrm{RC4}(V, K)) \oplus \mathrm{RC4}(V, K)=P$；

3）检验校验和。接收方根据恢复的明文信息 P' 来检验校验和。将 P' 分离成 $[M', c']$ 的形式，重新计算校验和 $c(M')$，并检查是否与接收到的校验和 c' 相匹配，这样可以保证只有正确的校验和数据帧才会被接收方接收。

2　WEP 安全漏洞

2.1　密码序列重复使用

流密码加密算法的一个缺陷：是如果用相同的 IV 和密钥加密 2 条消息易导致 2 条消息的同时泄漏。

例如：$C_1=P_1 \oplus \mathrm{RC4}(V, K)$，$C_2=P_2 \oplus \mathrm{RC4}(V, K)$，则有：

$C_1 \oplus C_2=(P_1 \oplus \mathrm{RC4}(V, K)) \oplus (P_2 \oplus \mathrm{RC4}(V, K))=P_1 \oplus P_2$。

从上式中可以看出 C_1 式和 C_2 式是接收到的 2 个不同密文消息，将它们进行异或运算后就能将密钥流去掉，结果是 2 个明文信息 P_1 和 P_2 的异或，假如其中 1 个消息的明文已知，不论另外 1 个信息是否可知，则它的明文都可以立即得到。

为阻止该类攻击，WEP 协议为每个分组采用不同的初始向量 IV 加以克服，避免密钥序列的重复。然而，无论是 40 bits 或 104 bits 长的密钥，其 IV 均为 24 bits，密钥空间只有 2^{24} 大小，对于 CCK 调制速率高达 11 Mbps 的情形，可能在 1 h 以后就出现重复。流加密算法本身的弱点以及 802.11 标准中初始向量空间太少，使密钥序列重复使用的机会大大增加，对于 WLAN 的安全是灾难性的[3]。

2.2　消息被篡改问题

WEP 协议使用 32 位的循环冗余校验（CRC−32）验证数据的完整性。这原本是通信中用于检查随机误码的，没有密码保护，并不具备抗恶意攻击所需的消息认证功能。它不能对付恶意攻击（malicious attack），具体分析如下：

设消息为 P，密文为 C，攻击者篡改数据为 D，篡改后的明文、密文分别为 P'、C'，则 $C=\mathrm{RC4}(V, K) \oplus <P, \mathrm{CRC32}(P)>$。由于 CRC32 不带密钥，因此攻击者可算得 CRC32(D)，现发起以下攻击：

$C \oplus (D, \mathrm{CRC32}(D))=\mathrm{RC4}(V, K) \oplus <P, \mathrm{CRC32}(P)> \oplus <D, \mathrm{CRC32}(D)>=$

$\mathrm{RC4}(V, K) \oplus <P \oplus D, \mathrm{CRC32}(P) \oplus \mathrm{CRC32}(D)>$，

攻击者完全可以不破坏校验和而对密文进行篡改。

2.3　密钥管理问题

在 802.11 标准中缺乏有效的密钥管理和分发机制，

由于分配给客户机的密码丢失或泄密等原因，威胁网络的安全。另外，密码的更换周期较长，攻击者有足够的时间利用统计攻击的方法获取它。

协议一般通过带外方式（out of band）分发密钥，通常标准分发4个密钥，每条消息中包含1个密钥标志符（key identifier）来表明其正在使用的密钥。标准也允许为每个移动台配置1个惟一的密钥，但这种选择往往不被广泛采用。实际使用时厂家经常为整个网络设置1个密钥，这样就带来了系统的安全隐患。另外，一旦网络规模扩大或者成员动态变化时，仍采用带外方式发布密钥工作量太大，而密钥的分发管理又直接关系到系统认证和加密的安全，如何动态地实施密钥管理与交换，并在无线环境下安全地进行密钥分发，都是急待解决的关键问题。

2.4 身份验证问题

如果WEP使用单向的身份验证，即接入点可以验证用户的身份，而用户不能反过来验证接入点是否就一定是自己想要连接的接入点，WLAN中就有可能混入1个虚假的访问点，它可以诱使合法的客户机作为自己发动攻击的平台[4]。

2.5 包头问题

WEP的包头没有加密，所以任何人可以看到数据传输的源和目的地址。

3 可发起的攻击

针对以上漏洞，对WEP算法采取以下攻击方式：

1）根据统计分析解密通信内容的被动攻击；

2）根据已知明文，从未授权无线站进入通信的主动攻击；

3）通过虚假AP实现解密主动攻击；

4）通过分析数目WLAN上的通信情况，允许实时自动地解密通信内容的字典构建攻击。

4 提高WLAN安全性的技术

针对802.11的安全问题，业内人士较多采用具有TKIP（Temporal Key Integrity Protocol）加密的802.1x认证和VPN数据加密技术，还有通过运用EAP等算法来增加无线传输的安全性。

4.1 具有TKIP加密的802.1x

802.1x定义受控和非受控2个逻辑端口，用于控制不同类型业务流的介入[5]。认证主要由申请者（Supplicant）、认证系统（Authenticator）、认证服务器系统（Authentication Server）3个部分组成。其中，申请者是申请接入的无线用户。认证系统在WLAN中就是AP，在认证完成前，它仅负责转发申请者的认证信息包。认证结束后，再向申请者提供无线接入服务。认证服务器系统存储有关用户的信息，比如用户所属的VLAN、口令、访问控制列表ACL等，为认证系统提供认证服务。

802.1x很好地解决了无线网络的身份认证问题，但它本身并不是加密算法，因此它仍然无法解决802.11中因WEP导致的安全缺陷，所以现在无线网络中常使用具有TKIP加密的802.1x。

暂时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）是专门用于纠正WEP脆弱性的协议，它仍然将RC4作为加密算法，但它强制每10 000个数据包或者10 kB（和数据源有关）就产生1个新密钥，其帧结构如图4。

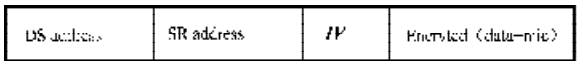

图4 TKIP帧结构

Fig. 4 TKIP encrypted frame

TKIP将密钥长度从40 bit增加到128 bit，根据临时密钥*TK*（128 bit）、TKIP序列计数器*TSC*（32 bit）和发送地址*TA*（48 bit）通过2个阶段动态生成，在通过认证结束后分配给申请者和认证系统使用，并形成配对密钥。每次认证过程产生的TKIP配对密钥都不同，每个TKIP配对密钥的泄漏也只会影响一对无线客户端和AP之间的通信安全，从而增加了安全性。

在认证之后的数据传输中，TKIP配对密钥和*IV*进行哈希运算，产生1个新的包密钥（packet key），数据包由包密钥加密后再加以发送。TKIP包密钥提供大约500万亿组的可能，从而使破解变得十分困难，而且TKIP在每个数据包中增加了1个消息集成检测MIC（Message Integrity Check）数值位，数据接收端会计算MIC数值位，并和数据包中的MIC数值位进行比较。从而确保数据包在发送后没有被篡改，也极大地提高了5项通信的安全性。

4.2 VPN数据加密技术

VPN（Virtual Private Network，虚拟专用网络）是在现有网络上组建的虚拟的、加密的网络。VPN主要采用隧道技术、密钥管理技术、访问控制技术、身份认证技术这4项来保障网络安全。

实现WLAN安全存取的层面和途径有多种。VPN的IPSec（Internet Protocol Necurity）协议是目前Internet通信中最完整的一种网络安全技术，利用它建立起来的隧道具有更好的安全性和可靠性。IPSec的加密技术基于DES（Data Encryption Standard，数据加密标准），长度为56 b；或者基于3DES（Triple DES，3重DES），即3 × 56=168 b。

4.3 EAP扩展认证协议

PPP扩展认证协议（EAP）是一个用于PPP认证的

通用协议，可以支持多种认证方法。EAP机制是基于IETF标准的，它不依赖于IP，它本身就是一个封装协议，可以运行任何链路层（PPP、802.3、802.5、802.11等）。EAP并不在链路建立阶段指定认证方法，而是把这个过程推迟到认证阶段。这样，认证方就可以在得到更多的信息以后再决定使用什么认证方法。这种机制还答应PPP认证方简单地把收到的认证报文透传给后方的认证服务器，由后方的认证服务器来真正实现各种认证方法。

1）在链路阶段完成以后，认证方向对端发送1个或多个请求报文。在请求报文中有1个类型字段用来指明认证方所请求的信息类型，例如是对端的ID、MD5的挑战字、一次密码（OTP）以及通用令牌卡等。MD5的挑战字对应于CHAP认证协议的挑战字。典型情况下，认证方首先发送1个ID请求报文，随后再发送其它的请求报文。当然，并不是必须要首先发送这个ID请求报文，在对端身份是已知的情况下（如租用线、拨号专线等）可以跳过这个步骤；

2）对端对每一个请求报文回应1个应答报文。和请求报文一样，应答报文中也包含1个类型字段，对应于所回应的请求报文中的类型字段；

3）认证方通过发送1个成功或者失败的报文来结束认证过程。

优点：EAP可以支持多种认证机制，而无需在LCP阶段预协商过程中指定。

某些设备（如：网络接入服务器）不需要关心每一个请求报文的真正含义，而是作为1个代理把认证报文直接透传给后端的认证服务器。设备只需关心认证结果是成功还是失败，然后结束认证阶段。

缺点：EAP需要在LCP中增加1个新的认证协议，这样现有的PPP实现要想使用EAP就必须进行修改。同时，使用EAP也和现有的在LCP协商阶段指定认证方法的模型不一致。

5　结语

安全问题仍将继续成为制约无线局域网产业发展的最大障碍。针对WEP的脆弱问题，WLAN安全方案也一直在不断发展。802.1x和VPN等技术虽然都能极大地提高无线网络的安全性和保密性，但是作为一种安全保密技术它们并不是无懈可击的，也不能弥补网络安全上的所有漏洞。在无线技术迅猛发展的今天，只有不断发展更新更完善的技术，才能构建更安全的无线网络。

参考文献：

[1] Andrew S，Tanenbaum. Computer Networks[M]. Fourth Edition. Beijing: Tsinghua University Press，2004:668-671.

[2] 苏　鹏，胡志远，塔维娜，等. 802.11无线局域网安全现状及其解决方案[J]. 计算机工程，2003，29(4)，112-114. Su Peng，Hu Zhiyuan，Taweina，et al. Present Security Condition of 802.11 Wireless LAN and Solution for the Vulnerabilities [J]. Computer Engineer，2003，29(4)，112-114.

[3] Tom Kevan. Wireless LAN Security[J]. Frontline Solutions Duluth，2003(4)：52.

[4] Prashnt K，Kabara J，Anusas-Amornkul T. Security in Wireless Residential Networks[J]. IEEE Transactions on Consumer Electronics，2002，48(1)：157-166.

[5] ANSI IEEE std 802.1X-2001. IEEE Standard for Local and Metropolitan Area Networks- Port-Based Network Access Control[S].

（责任编辑：罗立宇）