综述与评论 Review and Comment

浅谈无线局域网安全技术的发展

王 磊，梁华庆
（中国石油大学（北京），北京 102249）

摘 要：无线局域网在当前的计算机网络体系中占据重要地位。介绍无线局域网安全发展概况和基于 IEEE802.11i 标准体系的 WLAN 安全机制，并对无线局域网的安全技术发展进行了展望。

关键词：无线局域网；安全技术；802.11i

中图分类号：TP393.0 **文献标识码**：A **文章编号**：1674-7720(2011)06-0001-02

Development of the wireless local area network

Wang Lei, Liang Huaqing
(China University of Petroleum, Beijing Campus, Beijing 102249, China)

Abstract: The wireless local area network (WLAN) is playing an important character in the current computer network system. This article introduces the development of WLAN security. The paper elaborates the security mechanism of wireless network based on IEEE802.11i, and looks forward to the future to the development of the wireless network information security.

Key words: WLAN; security; 802.11i

802.11 采用 WEP 加密用来保证 WLAN 空中接口的数据安全，但是实际应用中 WEP 很容易受到攻击，无法提供类似于有线介质的安全性，2001 年 7 月 WEP 中的 RC4 加密技术被成功破解。这样，原本就不太安全的无线局域网变得更脆弱不堪。因此 IEEE 制定了 802.11i，用于增强 AP 的安全性，解决 WEP 加密的缺陷。

1 WEP

WEP 算法的主要目的是提供数据的完整性和物理层的保密性，并通过拒绝所有非法 WEP 信息包来拒绝对网络的非法访问。WEP 采用对称性加密算法 RC4，在加密与解密端均使用同样的 40 bit 长的密钥。密钥将会被发送到每一个终端以及访问点之中。WEP 也具有终端的认证功能，当加密机制功能启用，终端要尝试连接到访问点时，访问点会发出一个测验包(Challenge Packet)给终端，终端再利用共享密钥将封包加密后送回访问点以进行认证比对，如果无误，才能获准存取网络的资源。WEP 使用的 RC4 算法是一次性密码本形式的加密算法(只有在密码本仅用一次的情况下，一次性密码本的安全性才有效)。根据 FLUHRER、MANTIN、SHAMIR 的研究结果表明 RC4 算法中的 KSA (Key Scheduling Algorithm)本身存在缺陷，窃听者通过收集的大量 IV 值进行统计分析来解密，继而访问网络[1]，因此窃听者能够相当简单地破译 WEP 加密的消息，从而获得对网络和数据的访问。在攻击 WEP 之前，非法攻击者会嗅探合法密钥，并且通过重放攻击收集初始向量，最终破解 WEP 加密[2]。

2 802.11i 标准

802.11i 协议，通过使用增强认证(EAP/802.1X/RADIUS)、密钥的动态建立与管理和增强加密(CCMP)等来加强无线网络的安全，从而克服由于 WEP 本身的弱点给无线网络安全带来的影响。802.11i 标准包括了用户认证(使用 802.1X)、密钥管理、多种数据封装加密机制。在数据加密算法方面，定义了 TKIP、CCMP 和 WRAP 等 3 种加密机制。其中 TKIP 采用 IEEE 802.11WEP 机制中的 RC4 作为核心加密算法。CCMP 机制基于 AES 加密算法和 CCM 加密鉴别方式，使得 WLAN 的安全程度大大提高，是实现强安全网络(RSN)的强制性要求。

2.1 802.1X 用户认证

为了在 802.11 网络中提供比 WEP 更好的认证和机密性。IEEE802.11i 协议定义了一个基于 IEEE802.1X 认证的强安全网络关联(RNSN)，认证过程包括 3 个实体：请求者、认证者和认证服务器。一个成功的认证意味着请求者和认证者相互认证身份并生成共享密钥用于加密传输数据。AP 是认证者，认证服务器可以与认证者结合在一起，也可以是单独的 RADIUS 服务器。通过一个安全的物理链路与认证者建立连接。

IEEE802.11i 协议认证的完整过程包括请求者和认证者之间的握手(相互安全能力的通知和 IEEE802.1X 会话)、认证者和认证服务器(即 RADIUS)之间的握手,以及请求者和认证服务器之间的握手(EAP-TLS)。通过认证者转发,这些握手、请求者和认证服务器彼此互相认证并生成一个共同的密钥,称为主会话密钥 MSK(Master Session Key)。认证服务器将 MSK 安全地传输给认证者,请求者和认证者利用 MSK 生成 PMK(Pairwise Master Key),用于随后临时会话密钥 PTK 的生成。上述操作通过 4 次握手功能实现。

在 4 次握手过程中,请求者和认证者基于事先双方共有的 PMK 和握手过程中的参数等,分别在各自一端生成 PTK。PTK 并没有在双方之间传输,所以其密钥的安全性得到很好的保证。在 4 次握手完成后双方利用 PTK 中的 TK 加密通信数据信息,保证了数据传输的安全性。每次 4 次握手过程所产生的 PTK 仅在接下来的一次会话过程中使用。当需要新的会话时,则要重新开始 4 次握手建立新的 PTK。这种动态密钥与管理方式大大加强了 WLAN 的通信安全。

2.2 TKIP

TKIP 是在 WEP 基础上改进的加密系统,安全等级有所提高。TKIP 仍然采用了 WEP 加密,但在 WEP 基础上增加了使用 MIC 进行完整性校验、支持对 MPDU 进行编号防止重放攻击、使用两级密钥混合功能防止基于 WEP 密钥的攻击。

相应的,TKIP 扩展了加密帧格式,相对于 WEP,增加了 EIV 和 MIC 域,其中 EIV 域用于重放保护,MIC 域用于报文完整性校验。MIC 在 MPDU 分片之前进行计算,紧跟在数据之后,并使用 TKIP 进行加密。IV 中的 EIV 标识用于指示帧的加密方式。如果为 1,则是 TKIP 加密;否则即是 WEP 加密。

从以上可以看到,TKIP 针对 WEP 算法的缺陷做出了相应的改进,但是 TKIP 算法只是一种过渡性的算法,更高级的算法已经呼之欲出,即 802.11 工作组 I 确定使用的算法 CCMP。

2.3 CCMP

CCMP 采用 AES 系统,是目前最安全的无线局域网解密系统,但是无法兼容老设备。CCMP 提供了加密、认证、完整性和重放保护。CCMP 基于 CCM(Counter-Mode/CBC-MAC)方式,该方式使用了 AES 加密算法,CCM(定义在 RFC 3610)方式结合了用于加密的 Counter Mode(CTR)与用于认证和完整性的加密块链接消息认证码。CCM 保护 MPDU 数据和 IEEE802.11iMPDU 帧头部分域的完整性。

所有在 CCMP 中用到的 AES 处理都使用一个 128 bit 的密钥和一个 128 bit 的数据块。CCM 是一个通用模式,它可以用于任意面向块的加密算法。CCM 有两个参数(M 和 L)。CCMP 使用以下值作为 CCM 的参数:

M=8;表示 MIC 是 8 B。

L=2;表示域长度位为 2 B,这有助于保持 802.11MPDU 的最大长度。

针对每个会话,CCM 需要有一个全新的临时密钥,CCM 也要求用给定的临时密钥保护的每帧数据有唯一的 nonce 值。CCM 是用一个 48 bit PN 实现的。对于同样的临时密钥可以重用 PN,这可以减少很多保证安全的工作。

CCMP 处理用 16 B,扩展了原来 MPDU 的容量,其中 8 B 为 CCMP 帧头,8 B 为 MIC 校验码。CCMP 帧头由 PN、ExtIV(扩展初始向量)和 Key ID 域组成。PN 是一个 48 bit 的数字,是一个 6 B 的数组。PN5 是 PN 的最高字节,PN0 是最低字节。值得注意的是,CCMP 不使用 WEP ICV。ExtIV 域表示 CCMP 扩展了帧头 8 B,如果使用 CCMP 加密,则 ExtIV 的值总为 1。这些设置更加确保了无线传输数据的真实性和安全性。

由此可知,CCMP 的安全性主要取决于 AES 算法和 CCM 操作模式,而 AES 和 CCM 的理论基础非常牢固,且都经过了网络安全领域众多专家和多年实践的检验,从目前情况看,CCMP 具有很高的安全性,已经逐渐在无线局域网安全产品中展开应用,在很长一段时期内将成为无线局域网最重要的安全机制。

本文主要介绍了 WLAN 技术发展以来所使用的安全技术,对不同阶段的安全机制进行了一定的分析,虽然 802.11i 标准带来了相对安全的无线网络环境,但是其核心算法 CCMP 无法兼容老设备。随着无线网络的发展和安全技术的不断进步,越来越健全的无线网络环境将会出现。

参考文献

[1] 陆波波,黄鸿,任雪梅,等.802.11 无线局域网安全与应用研究[J].微计算机信息,2005,21(5):226-227.

[2] 张园,王青松.无线局域网安全技术综述[J].计算机与现代化,2008(11):28-30.

(收稿日期:2010-11-27)

作者简介:

王磊,女,1984 年生,在读研究生,主要研究方向:软件开发与测试。

梁华庆,女,1964 年生,教授,博士生导师,主要研究方向:石油生产过程的信号检测与处理、石油测井仪器的研发和信息安全。