

基于 802.11i 的 WLAN 动态密钥管理机制分析及改进

赵伟艇

(平顶山学院,河南 平顶山 467000)

摘 要: 介绍了新一代 WLAN 安全标准 802.11i,研究了 802.11i 协议的动态密钥管理机制,从四步握手角度对其安全性进行了深入分析,指出了可能受到的 DoS 攻击.提出了两种改进设计方案,有效避免了这些攻击,进一步完善了无线局域网的安全性能.

关键词: 无线局域网;IEEE802.11i;密钥管理

中图分类号: TP393.17

文献标识码: A

文章编号: 1000-7180(2010)04-0193-05

Analysis and Improvement of Dynamic Key Management Based on WLAN 802.11i

ZHAO Wei-ting

(Pingdingshan University, Pingdingshan 467000, China)

Abstract: The WLAN's new generation of security standard IEEE 802.11i protocol is introduced, and the dynamic key management based on 802.11i was discussed, and its security is also analysed deeply from the 4-Way Handshake Protocol, then the possible Denial of Service attacks are indicated. To deal with these attacks, two improved measures were put forward to enhance the WLAN's security.

Key words: WLAN; IEEE802.11i; key management

1 引言

无线局域网(WLAN)以其灵活的组网方式在校园、办公室、科研机构等众多场得到了广泛的应用,但由于其完全暴露在外的传输媒介使得无线网络比有线网络更容易受到攻击,其安全问题影响着无线网络的发展^[1-5].

新一代安全标准 IEEE 802.11i 通过使用增强认证(EAP/802.1x/RADIUS)、密钥的动态建立与管理并增强加密(CCMP)等极大地提高了无线网络的安全性能,但仍然存在局限性及可能的攻击威胁^[6-9].文中对 802.11i 的动态密钥管理机制的安全性进行了分析,并针对其安全缺陷进行了改进设计,进一步完善了 WLAN 的安全性能.

2 IEEE 802.11i 协议概述

IEEE 802.11i 协议标准共包括 3 部分^[4,6-8],可分为 2 个层次,下层是 3 种改进的加密协议,即 TKIP、CCMP 和 WRAP,实现数据的加密和安全传输,上层是 802.1x 协议和 EAP 认证协议,提供双向认证和动态密钥管理功能,其协议栈结构如图 1 所示.

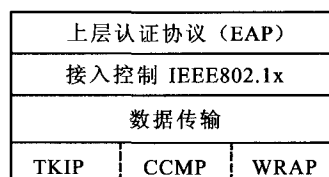


图 1 IEEE 802.11i 协议栈

IEEE 802.11i 定义了强健安全网络关联

(RSNA)的概念,其目标是实现数据机密性、身份识别、接入控制、抗重放攻击、数据完整性校验.其中,机密性和数据完整性校验以及抗重放攻击由 TKIP 或者基于 AES 算法的 CCMP 一次性实现,RSNA 实现了身份识别和接入控制以及密钥管理这几个目标.RSNA 的运行机制由安全能力发现、身份认证与访问控制、密钥分发及管理、加密数据传输四部分组成.具体实现流程如图 2 所示.

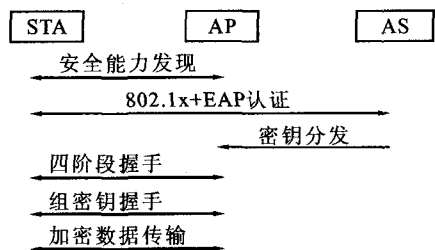


图 2 RSNA 工作流程

- 安全能力发现:该阶段在 STA 与 AP 之间建立 802.11 关联,每个 AP 使用 Beacon 信标报文将可提供的安全措施,如支持怎样的认证方式或报文加密算法等封装在 RSN IE(RSN Information Element)结构中,并定期向其辐射范围内的所有客户端广播该报文,客户端收到若干这样的安全能力宣告报文后选定一个 AP 作为接入点,并使用 Probe 探测报文与 AP 完成交互建立关联,在此基础上 STA 开始同 AS 进行真正的认证过程.

- 认证和访问控制:该阶段是围绕着 IEEE802.1x 来实现的,主要任务是确定 STA 和 AS 的身份.其中 STA 与 AP 之间的报文交互在无线 802.11 环境中完成,故采用 EAPOL (EAP over LAN)协议传输,而 AP 与 AS 之间的报文传递在有线网络中完成,可以采用 RADIUS 协议,具体的认证方式由 EAP-TLS 协议提供.802.11i 中实现了客户端同 AS 的相互身份认证,一旦认证通过,AS 与客户端将同时拥有 EAP 主密钥 (Master Key, MK),并由此产生 STA 访问 WLAN 的成对主密钥 (Pairwise Master Key, PMK),该密钥同时由 AS 通过 AS 与 AP 之间的安全通道发布给与 STA 关联的 AP.

- 密钥管理(Key Management):该阶段主要任务是产生 STA 与 AP 通信所使用的密钥,具体过程是通过四步握手协议和组密钥握手实现的.

- 数据安全传输:该阶段由 AP 与 STA 选择一定的加解密算法都使用密钥进行加密通信,相当于在 AP 与 STA 之间建立了一条安全通道.

3 802.11i 动态密钥管理

密钥管理技术是安全系统实施的基础,它能够在授权方向建立密钥关系并且加以维护.密钥是保密系统中最脆弱,也是最重要的环节,密钥的安全可以说是整个安全系统的核心,在 IEEE802.11i 标准协议中采用了基本上遵循 EAP 的密钥管理框架,动态密钥发放和更新机制是设计的一个重点^[2-5],动态密钥管理可以在很大程度上保证密钥的安全.

3.1 802.11i 的密钥管理系统

802.11i 的密钥管理系统中有三个逻辑实体:申请者(STA)、认证者(AP)和认证服务器(AS).当申请者和认证服务器通过相互认证,创建了一个安全的通道并产生一个主密钥后,就进入密钥管理流程.

(1) 申请者和认证服务器之间采用 IEEE802.1x 的 EAP-TLS 认证方法,通过相互认证,产生一个 32 字节的 EAP 主密钥,并通过各自的 EAP 主密钥产生成对主密钥,该密钥同时由认证服务器通过 RADIUS 协议创建的安全通道传递给认证者端.

(2) 申请者和认证者之间采用四步握手协议传送 EAPOL-Key 消息,来确保 PMK 的存在性,并由 PMK 产生成对临时密钥 (Pairwise Transient Key, PTK),按照需要加载加密/整体性校验机制.

(3) 认证者向申请者发送组临时密钥 (Group Transient Key, GTK),以允许申请者传送和接收广播消息,并且能够选择性地向认证者发送单播数据包.这类消息也采用 EAPOL-Key 进行封装.

3.2 密钥层次与派生

802.11i 协议中 EAP 认证成功后,STA 和 AS 生成了主密钥 MK,再由伪随机函数 (Pseudo-Random Function, PRF)派生出 PMK,并由 AS 传递给 AP.AP 和 STA 通过四阶段握手机制由 PRF 函数派生出 PTK,再把该密钥分成几部分得到加密所需的各种密钥供加密模块使用.组密钥握手可派生出新的 GTK,以保障组播数据的安全.密钥的层次与派生过程如图 3 所示.

密钥派生中使用的 PRF 函数是基于 SHA1 哈希算法和 HMAC 算法的伪随机函数,生成 PTK 的参数 AA 和 SA 分别是认证者和申请者的 MAC 地址;SNonce 和 ANonce 分别是申请者和认证者发出的随机数当前值.在采用 CCMP 协议进行数据的加密通信时导出的 PTK 为 384 位,而在采用 TKIP 协议进行数据加密通信时 PTK 为 512 位.

为保证数据传输的安全,802.11i 中 PTK 按用

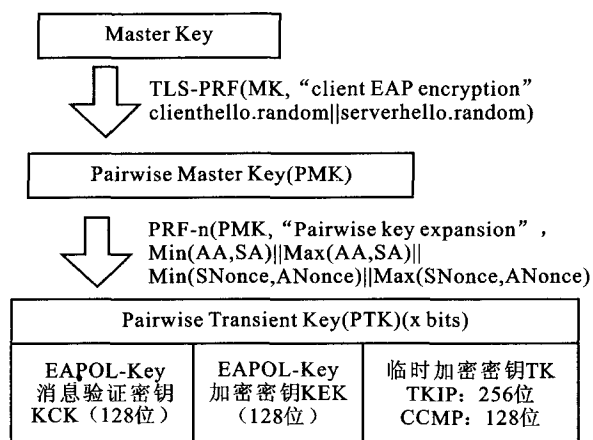


图3 密钥层次与派生

途可以分为多种密钥: 密钥信息完整性验证密钥(Key Confirmation Key, KCK), 密钥信息加密密钥(Key Encryption Key, KEK), 数据临时加密密钥(Temporal Key, TK), 数据完整性验证密钥(TKIP MIC Key, TMK), 如图4所示. KCK用于在进行密钥分发的过程(四步握手和组密钥握手过程)中, 对AP及STA发送的协议数据进行认证, 防止对协议数据的伪造和篡改. KEK用于在进行组播密钥分发时加密GTK, 确保GTK只有合法用户才能收到. TK是在802.11数据通信时用于加密数据帧的临时密钥, 在使用CCMP作为数据加密协议时, 加密密钥为128位, 而在采用TKIP作为数据加密协议时, 除了128位的加密密钥外, 还使用了两个64位的密钥作为TKIP MIC密钥, 用于保护发送的数据, 验证发送方的身份. 其中Rx Key用于接收方(STA)MIC校验, Tx Key用于发送方MIC校验.

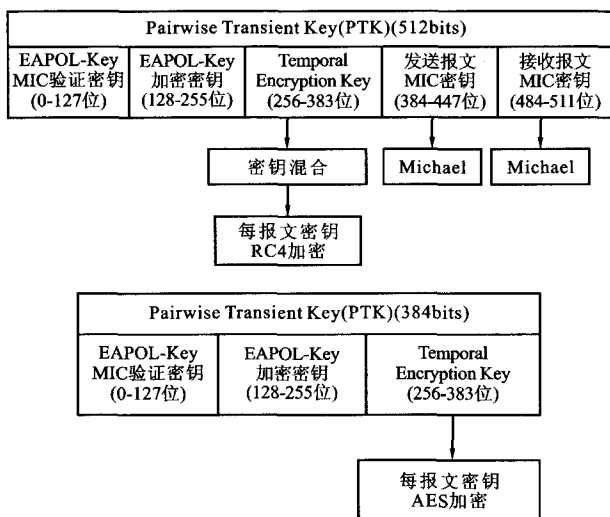


图4 TKIP和AES的密钥构成

3.3 四步握手密钥协商机制

四步握手协议用来在AP和STA之间生成并管理PTK的交互过程, 通过握手两者将产生用于报文加密、完整性校验等各种安全措施的密钥, 因此四步握手是密钥管理系统中至关重要的步骤, 其流程如图5所示.

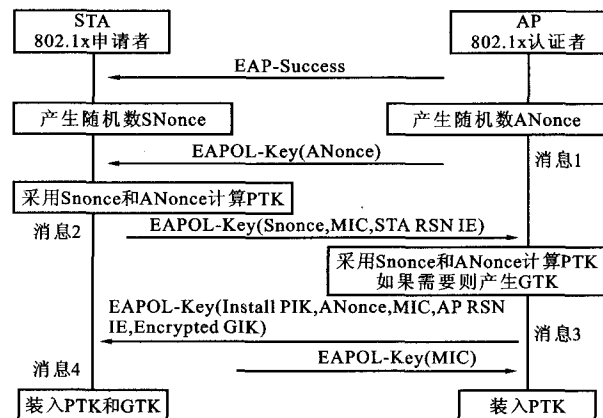


图5 四步握手过程

(1) AP向STA发送EAPOL-Key消息, 其中包含用于产生PTK的随机数ANonce. 该消息以明文形式发送, 由于无法生成PTK, 也没有对报文使用MIC完整性校验.

(2) STA收到消息后, 得到ANonce, 自行生成随机值SNonce, 使用ANonce、SNonce、STA与AP的MAC地址和PMK为输入调用PRF-n伪随机函数生成PTK, 然后向AP发送EAPOL-Key消息, 其中包含Snonce, STA的RSN IE, 并用KCK对消息做MIC校验.

(3) AP收到消息2后, 同样调用PRF-n伪随机函数生成PTK, 并对消息2做MIC校验, 如果校验失败就丢弃消息2, 正确则将消息2中的STA RSN IE与STA在与AP建立关联时发送的RSN IE进行比较, 如果不同, 则中断与STA的关联; 如果相同, 则向STA发送EAPOL-Key消息, 其中包含ANonce, AP自己的RSN IE, MIC及是否安装加密/整体性密钥. 另外, 组播密钥GTK经加密后也由该消息一并传送至STA端.

(4) STA收到消息3并校验正确后即装入PTK, 并发送EAPOL-Key消息, 确认密钥已经安装, AP收到消息4并校验正确后也装入PTK, 四步握手完成.

3.4 组密钥握手机制

组密钥握手机制用来向申请者发送新的组密钥, 只有当第一次四步握手成功后才能进行组密钥

初始化,流程如图 6 所示.

(1)认证者产生新的 GTK 并对其加密,包含在 EAPOL-Key 消息中发送.

(2)申请者对收到的消息做 MIC 校验,解密 GKT 并安装到加密/整体性机制中,并发送 EAPOL-Key 消息,对认证者进行确认.

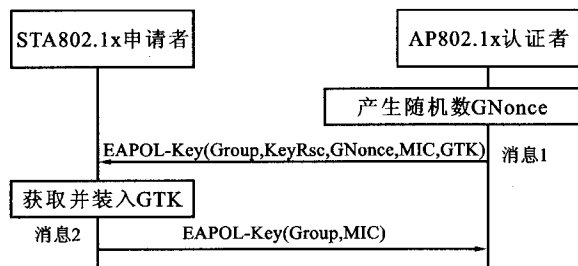


图 6 组密钥握手过程

4 密钥管理安全性分析

IEEE802.11i 的安全关联实质上是 STA、AP 和 AS 间相互认证的过程^[1,8],三者间的安全会话是整个密钥生成的基础.由于所采用的 EAP 认证方法(如 802.11i 默认的 EAP-TLS)有足够的安全性,且 MK 是不容易攻破的,也不向第三方透露,整个密钥的基础是安全的.因此 IEEE802.11i 中密钥管理的安全性取决于四步握手的安全性.

4.1 四步握手的安全性

四步握手的目的在于由 STA 和 AP 共享的 PMK 推导单播通信密钥 PTK.四步握手以 PMK 为信任基础^[1],双方分别提供了随机数和 MAC 地址,可以保证握手报文的现场性以及协商所得会话密钥的新鲜性.握手报文带有验证码 MIC,可防攻击者篡改.组密钥握手由 PTK 推导的两个密钥保证组密钥分发报文的完整性和保密性,并用密钥序列号防止重放攻击;四次握手中还考虑了对无线链路连接的探寻阶段协商的密码算法进行有保护的确认,总体而言,四步握手具有较好的安全性.

4.2 可能受到的攻击

四步握手机制虽然是安全的,但在可用性方面却存在拒绝服务(DoS)漏洞.四步握手过程中,考虑到可能会发生丢包和重发的情况,申请者必须保留它所收到的所有消息 1 数据包以保证握手过程的完成.消息 1 没有使用任何加密或完整性校验措施,攻击者只要知道 STA 和 AP 的 MAC(这可以直接通过检测网络数据得到),很容易假冒 AP 伪造消息 1.攻击者在正常的消息 1 和消息 3 之间发送带有不同 Nonce 值的伪造的消息 1,从而导致申请者与认证者

之间 PKT 的不一致.为了存放这些伪造的消息 1,申请者不得不保存所有相应的 Nonce 值和派生的 PKT,只有在有效的消息 3 收到之后,申请者才能够安装相应的正确的 PTK 用于数据的传送,而丢弃所有不正确的 PKT.显然攻击者可以通过发出无数伪造的消息 1,造成 STA 的内存耗尽,形成 DoS 攻击.这一攻击也是很严重的,因为攻击者发起这样的攻击非常容易,而且这一攻击一旦成功,就会使之前所有的认证过程付诸东流.

4.3 改进方案

针对四步握手过程中遇到的 DoS 攻击,可采取如下的两种改进方案:

方案 1: 重用 SNonce

重用 Nonce 方法旨在消除 STA 端存在的中间状态,即 STA 在一次成功的四步握手过程完成之前针对不同的消息 1 重复使用第一次生成的 SNonce 计算 PTK 并形成消息 2 的 MIC 校验后发送消息 2,但不存储相应的 PTK,而是在收到消息 3 后重新计算 PTK 进行校验,如果校验成功则装入该 PTK,用于本次会话的数据加密,否则终止该握手过程.也就是 STA 在接收并认证消息 3 之前,重复使用同一个 Snonce 来对每一个接收到的消息 1 予以响应.这个改进的方法不用再缓存收到的每一个 ANonce 及对应生成的 PTK,很好地避免了存储器资源被耗尽所造成的 DoS 攻击.

方案 2: 对消息 1 进行身份认证

对四步握手协议的攻击是由于消息 1 缺少认证,攻击者伪造消息 1 引起的.只要在消息 1 中加入身份认证,确认消息 1 是由 AP 发送的,而不是由其他人伪造的,就可消除 DoS 攻击.四次握手是在认证成功时触发的,此时 STA 和 AP 拥有相同的成对主密钥 PMK,而且 PMK 只被 STA 和 AP 所拥有,因而,消息 1 的身份认证可以用 PMK 通过对称加密技术实现.首先 AP 使用 PMK 加密生成的随机值 ANonce,然后在消息 1 将该加密后的 ANonce 值放入 EAP-TLS 的 Key Data 字段中并发送给 STA.当 STA 收到消息 1 后,使用其拥有的 PMK 将加密的 ANonce 解密后与未加密的 ANonce 进行比较,如果不一致则直接丢弃该消息 1,否则认为是合法 AP 发送的消息,STA 会用该 ANonce 计算新的 PTK,其后的三个消息传送过程和 802.11i 标准中的四次握手协议完全相同.该方案中攻击者由于无法知道用于加密的 PMK 密钥和加密算法,生成的伪造消息已毫无意义,这种方法只修改了消息 1,不对整个

协议进行修改,因此额外开销比较少,易于在已经部署了 802.11i 设施的构件中升级.

5 结束语

802.11i 标准提供了较为完整的动态密钥管理机制,通过四步握手协议为 STA 和 AP 协商临时会话密钥提供了每次会话的安全性.但协议中的设计缺陷使它容易遭受 DoS 攻击,文中从降低协议遭受攻击的发生入手,给出了两种改进设计方案,较好地避免了 DoS 攻击.在改进协议安全性的同时如何提高执行效率,是需要进一步研究的内容之一.

参考文献:

- [1] 王小军,陆建德.基于 802.11i 四次握手协议的攻击分析与改进[J].计算机工程,2007,33(2):171.
- [2] 王曼珠,何文才,杨亚涛,等.无线局域网 IEEE 802.11 的安全缺陷分析[J].微电子学与计算机,2005,22(7):189-192.
- [3] 孙树峰,贺樑,石兴方,等.802.11 无线局域网安全技术研究[J].计算机工程与应用,2003,39(7):40-42.

- [4] Sithirasanen E, Muthukkumarasamy V. An early warning system for IEEE 802.11i wireless networks [C]// AusWireless'06: Proceedings the of 1st Australian Conference on Broadband Wireless and Ultra Wideband. Australian, 2006:25-30.
- [5] 张文革,马玉祥.基于 OPNET 的 IEEE802.11 战场 WLAN 增援救助仿真及性能评估[J].微电子学与计算机,2006,23(2):42-44.
- [6] Tim Moore. Suggested changes to robust security network (RSN) for IEEE 802.11[R]. IEEE P802.11 Task Group I Meeting Update, 2002.
- [7] 苏鹏,胡志远.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.
- [8] Sithirasanen E, Muthukkumarasamy V, Powell D. IEEE 802.11i WLAN security protocol - a software engineer's model[C]// AusCERT'05: Proceedings of the 4th Asia Pacific Information Technology Security Conference. Sydney, 2005:39-50.

作者简介:

赵伟艇 男,(1966-),副教授.研究方向为计算机网络安全、网络管理等.

(上接第 192 页)

参考文献:

- [1] Khaled labid, Rao Venuri V. Application of principal component analysis to the detection and visualization of computer network attacks[C]// Annals of Telecommunications. France, 2005.
- [2] 朱永宣.入侵检测系统中基于主成份分析特征提取研究[J].微电子学与计算机,2006,23(7):91-96.
- [3] 张家超,孔媛媛.结合 SVM 与免疫遗传算法设计 IDS 的检测算法[J].微电子学与计算机,2008,25(10):206-209.
- [4] 徐耀红.数据融合理论与应用[M].西安:西安电子科技大学出版社,1998.

- [5] 孙即祥.现代模式识别[M].北京:国防科技大学出版社,2003.
- [6] Ludmila I. Kuncheva. A theoretical study on six classifier fusion strategies[J]. IEEE Trans On PAMI, 2002, 24(2):281-286.

作者简介:

张瑞霞 女,(1973-),硕士,讲师.研究方向为计算机信息与网络安全、入侵检测等.

王勇 男,(1964-),博士,教授.研究方向为信息安全、智能入侵检测等.